

PROJEKT WYKONAWCZY



**BUDOWA BUDYNKU SIEDZIBY DLA PROKURATURY REJONOWEJ W
GRODZISKU MAZOWIECKIM PRZY UL. BARTNIAKA WRAZ Z
NIEZBĘDNĄ INFRASTRUKTURĄ, ZAGOSPODAROWANIEM,
PODZIEMNYM ZBIORNIKIEM P.POŻ., PODZIEMNYM ZBIORNIKIEM NA
WODĘ, WIATĄ ŚMIETNIKOWĄ, WIATĄ ROWEROWĄ, PARKINGAMI**

TOM 6/16

PROJEKT INSTALACJI TELETECHNICZNYCH

KATEGORIA OBIEKTU XII, XXVI



Lokalizacja:	Grodzisk Mazowiecki przy u. Bartniaka, dz. 11/5 obręb 0029 identyfikator działki 140504_4.0029.11/5
Inwestor:	Skarb Państwa – Prokuratura Okręgowa w Warszawie ul. Chocimska 28, 00-791 Warszawa
Pracownia projektowa:	Konopińscy sp. z o.o. ul. Ciepelowska 10 04-967 Warszawa

Data: 10.07.2023 / 24.11.2023

Egz nr.

Załącznik do strony tytułowej

Projekt wykonawczy dla budowy budynku siedziby dla Prokuratury Rejonowej w Grodzisku Mazowieckim przy ul. Bartniaka wraz z niezbędną infrastrukturą, zagospodarowaniem, podziemnym zbiornikiem p.poż., podziemnym zbiornikiem na wodę, wiatą śmietnikową, wiatą rowerową, parkingami opracował zespół projektowy w składzie:

imię i nazwisko	funkcja / uprawn.	branża	podpis
mgr inż. Sławomir Radziszewski specjalność elektryczna	projektant MAZ/0540/POOE/14	instalacyjna elektryczna	
mgr inż. Mirosław Konca specjalność elektryczna	sprawdzający CIE13/86	instalacyjna elektryczna	

Spis zawartości projektu wykonawczego:

TOM 1 – Projekt dróg i zagospodarowania terenu
TOM 2 – Projekt architektoniczny
TOM 3 – Projekt konstrukcyjny
TOM 4 – Projekt SUG
TOM 5 – Projekt instalacji elektrycznych
TOM 6 – Projekt instalacji teletechnicznych
TOM 7 – Projekt instalacji SSP
TOM 8 – Projekt oddymiania klatki schodowej
TOM 9 – Projekt instalacji centralnego ogrzewania oraz ciepła technologicznego
TOM 10 – Projekt instalacji wodno-kanalizacyjnych
TOM 11 – Projekt instalacji chłodniczych
TOM 12 – Projekt wentylacji mechanicznej oraz klimatyzacji
TOM 13 – Projekt instalacji gazu oraz gazowych pomp ciepła
TOM 14 – Projekt zewnętrznych instalacji wodno-kanalizacyjnych
TOM 15 – Projekt zjazdu
TOM 16 – Operat pożarowy

Spis treści

I.	Część opisowa	4
1	Charakterystyka budynku	5
2	Wypożyczenie obiektu w instalacje	5
3	Podstawa opracowania	5
4	Instalacja teletechniczna	6
4.1	Okablowanie strukturalne	6
4.2	Wymagania ogólne okablowania	7
4.3	Rozprowadzenie instalacji	10
4.4	Pomiary Okablowania Miedzianego	12
4.5	Pomiary okablowania światłowodowego	12
4.6	Dane techniczne urządzeń aktywnych	12
4.7	Instalacja CCTV	17
4.8	Opis zastosowanych kamer	17
4.9	Serwer zarządzania i rejestracji	20
4.10	Stacja robocza:	21
5	Instalacja Kontroli Dostępu	21
6	Instalacja SSWiN	32
7	Rozłączanie klimatyzacji po otwarciu okna	40
8	Access Point Wi-Fi	42
9	Wideodomofon	43
10	Instalacja przyzywowa	46
11	BMS 46	
12	Kanalizacja teletechniczna	54
13	Warunki techniczne przyłączenia do sieci teletechnicznej	56
II.	Część rysunkowa	59
III.	Dokumenty formalno-prawne	75
1	Oświadczenie Projektantów	76
2	Uprawnienia i zaświadczenia	77
3	Decyzja na lokalizację urządzeń w pasie drogi teletechnika	83
4	Pismo uzgodnienia przyłącze teletechnicznego Orange	90
5	Uzgodnienie przyłącze teletechnicznego Orange	93

Spis rysunków

T01 - Parter - Rzut instalacji teletechnicznej, kontroli dostępu, wideodomofonu i przyzywowej	60
T02 – 1 Piętro - Rzut instalacji teletechnicznej, kontroli dostępu, wideodomofonu i przyzywowej	61
T03 – 2 Piętro - Rzut instalacji teletechnicznej, kontroli dostępu, wideodomofonu i przyzywowej	62
T04 - Schemat instalacji wideodomofonu	63
T05 - Schemat okablowania strukturalnego. Szafa GPD	64
T06 - Schemat okablowania strukturalnego. Szafa GPD2	65
T07 - Schemat okablowania strukturalnego. Szafa LPD1	66
T08 - Schemat instalacji przyzywowej	67
T09 - Schemat instalacji kontroli dostępu KD	68
T10 - Ogólny schemat struktury sieci teletechnicznej i BMS	69
T11 - Parter - Rzut instalacji alarmowej SSWiN i CCTV	70
T12 - 1 Piętro - Rzut instalacji alarmowej SSWiN i CCTV	71
T13 - 2 Piętro - Rzut instalacji alarmowej SSWiN i CCTV	72
T14 - Schemat instalacji alarmowej SSWiN1 i SSWiN2	73
T15 - Schemat instalacji monitoringu CCTV	74

I. Część opisowa

1 Charakterystyka budynku

Przedmiotem opracowania jest projekt wykonawczy instalacji teletechnicznej budynku PROKURATURY REJONOWEJ W GRODZISKU MAZOWIECKIM PRZY UL. BARTNIAKA WRAZ Z NIEZBĘDNĄ INFRASTRUKTURĄ I ZAGOSPODAROWANIEM

2 Wyposażenie obiektu w instalacje

Projekt budynku obejmie następujące instalacje:

- Instalacja alarmowa SSWiN
- instalacja teletechniczna
- Okablowanie strukturalne
- Instalacja kontroli dostępu KD
- Instalacja monitoringu CCTV
- Instalacja BMS
- Instalacja wideodomofonu
- Instalacja przyzywowa

3 Podstawa opracowania

Podstawą opracowania projektu budowlanego jest Umowa Nr 3041-7.261.2022 zawarta pomiędzy Skarbem Państwa – Prokuraturą Okręgową w Warszawie z siedzibą w Warszawie (00-791) przy ulicy Chocimskiej 28 (NIP 525-10-08-711; Regon 000000247) w Warszawie, a pracownią projektową Konopińscy Sp. z o.o. z siedzibą w Warszawie 04-967 przy ul. Ciepłowskiej 10 (NIP 952-221-84-29; Regon 389412706).

Normy i przepisy związane:

- Ustawa z dnia 7 lipca 1994r., - Prawo budowlane (Dz. U. Nr 89, poz. 414, z późniejszymi zmianami),
- Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 roku w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz. U. z 2002 Nr 75 poz. 690), z późniejszymi zmianami,
- Rozporządzenie Ministra Infrastruktury z dnia 6 lutego 2003 r w sprawie bezpieczeństwa i higieny pracy podczas wykonywania robót budowlanych (Dz. U. z dn. 19.03.2003 r. Nr 47, poz.401)
- Rozporządzenie Ministra Rozwoju i Technologii z dnia 20 grudnia 2021 r. w sprawie określenia metod i podstaw sporządzania kosztorysu inwestorskiego, obliczania planowanych kosztów prac projektowych oraz planowanych kosztów robót budowlanych określonych w programie funkcjonalno-użytkowym (Dz.U. 2021 poz. 2458).
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 nr 109 poz. 719).
- Ustawa o wyrobie budowlanym z 16.04.2004 (DZ.U. nr 92/2004 poz. 881)
- Rozporządzenie Ministra Infrastruktury i Budownictwa z dnia 17 listopada 2016 r. w sprawie sposobu deklarowania właściwości użytkowych wyrobów budowlanych oraz sposobu znakowania ich znakiem budowlanym (Dz.U. 2016 poz. 1966).

- Rozporządzenie Ministra Budownictwa i Przemysłu Materiałów Budowlanych z dnia 28 marca 1972 r. w sprawie bezpieczeństwa i higieny pracy przy wykonywaniu robót budowlano-montażowych i rozbiórkowych (Dz.U. 1972 nr 13 poz. 93).
 - Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 26 września 1997 r w sprawie ogólnych przepisów bezpieczeństwa i higieny pracy (Dz.U. 1997 nr 129 poz. 844).
 - Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 14 marca 2000 r. w sprawie bezpieczeństwa i higieny pracy przy ręcznych pracach transportowych (Dz.U. 2000 nr 26 poz. 313).
 - A także: wymagania i badania przy odbiorze oraz inne obowiązujące PN (EN-PN) lub odpowiednie normy krajów w zakresie przyjętym przez polskie prawodawstwo.
- PN-HD 60364-1:2010/A11:2017-10 Instalacje elektryczne niskiego napięcia -- Część 1: Wymagania podstawowe, ustalanie ogólnych charakterystyk, definicje
- PN-HD 60364-4-41:2017-09 Instalacje elektryczne niskiego napięcia -- Część 4-41: Ochrona dla zapewnienia bezpieczeństwa -- Ochrona przed porażeniem elektrycznym
- PN-IEC 60364-5-52:2011 Instalacje elektryczne niskiego napięcia -- Część 5-52: Dobór i montaż wyposażenia elektrycznego -- Oprzewodowanie
- PN-HD 60364-5-53:2022-10 Instalacje elektryczne niskiego napięcia -- Część 5-53: Dobór i montaż wyposażenia elektrycznego -- Aparatura rozdzielcza i sterownicza
- PN-HD 60364-5-54:2011 Instalacje elektryczne niskiego napięcia -- Część 5-54: Dobór i montaż wyposażenia elektrycznego -- Układy uziemiające i przewody ochronne
- PN-IEC 60364-6:2016-07 Instalacje elektryczne niskiego napięcia -- Część 6: Sprawdzanie
- PN-EN 50130-4:2012 Systemy alarmowe -- Część 4: Kompatybilność elektromagnetyczna -- Norma dla grupy wyrobów: Wymagania dotyczące odporności urządzeń systemów sygnalizacji pożarowej, sygnalizacji włamania, sygnalizacji napadu, CCTV, kontroli dostępu i osobistych
- PN-EN 62676-1-2:2014-06 Systemy dozoru CCTV stosowane w zabezpieczeniach -- Część 1-2: Wymagania systemowe -- Wymagania eksploatacyjne dotyczące transmisji wizji
- PN-EN 62676-3:2015-11 Systemy dozoru wizyjnego stosowane w zabezpieczeniach -- Część 3: Analogowe i cyfrowe interfejsy wizyjne
- PN-EN 62676-4:2015-06 Systemy dozoru wizyjnego stosowane w zabezpieczeniach -- Część 4: Wytyczne stosowania
- PN-EN 50131-1:2009 Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 1: Wymagania systemowe
- PKN-CLC/TS 50131-7:2011 Systemy alarmowe -- Systemy sygnalizacji włamania i napadu -- Część 7: Wytyczne stosowania
- PN-EN 60839-11-15 Systemy alarmowe i elektroniczne systemy zabezpieczeń -- Część 11-1: Elektroniczne systemy kontroli dostępu -- Wymagania dotyczące systemów i komponentów
- PN-EN 50173-1:2018-07 Technika informatyczna -- Systemy okablowania strukturalnego -- Część 1: Wymagania ogólne

4 Instalacja teletechniczna

4.1 Okablowanie strukturalne

W budynku zostanie zaprojektowana sieć strukturalna w oparciu o okablowanie miedziane oraz światłowodowe.

Cały budynek wyposażony będzie w okablowanie szkieletowe. W pomieszczeniu na parterze zlokalizowany zostanie Główny Punkt Dostępowy (GPD), do którego doprowadzone zostaną lokalne punkty dystrybucyjne (GPD2) oraz (LPD1) zlokalizowane w serwerowni na 2 piętrze i w

pomieszczeniu archiwum w kancelarii tajnej. Wymagane okablowanie musi być wykonane co najmniej kablami U/FTP 6A. Wszystkie szafki GPD połączone są ze sobą za pomocą kabla światłowodowego. Przewody sieci komputerowej będą zakończone w szafie rack min. 24U i rozszyte na patchpanelu. Zasilenie szaf crosowych będzie doprowadzone z wydzielonych obwodów elektrycznych.

Przewody prowadzić w przestrzeni sufitu podwieszanego w korycie kablowym lub w rurkach ochronnych podtynkowo w zależności od konstrukcji stropu.

W lokalnym punkcie dystrybucyjnym umieszczone zostaną aktywne urządzenia LAN takie jak przełączniki, zasilacze.

Projektuje się wykonanie za pomocą przewodu co najmniej kategorii 6a U/FTP klasy EA zakończonego złączami typu keystone. Okablowanie będzie jednolite dla sieci strukturalnej oraz systemu telewizji dozorowej. Zaleca się aby okablowanie szafy i osprzęt pochodziły od jednego producenta.

Instalacja teletechniczna składa się z następujących szaf:

- GPD - Główna szafa dystrybucyjna (parter)
- GPD2 - Pośredni punkt dystrybucyjny (Serwerownia)
- LPD1 - Pośredni punkt dystrybucyjny (Kancelaria tajna)

4.2 Wymagania ogólne okablowania

Wymagania ogólne dotyczące systemu okablowania strukturalnego System okablowania strukturalnego ma zapewnić niezawodną i wydajną warstwę fizyczną sieci teleinformatycznej, która zagwarantuje wystarczający zapas parametrów transmisyjnych dla działania dzisiejszych i przyszłych aplikacji transmisyjnych. W celu spełnienia najwyższych wymogów jakościowych i wydajnościowych należy zapewnić:

- Okablowanie miedziane co najmniej kategorii 6A (klasy EA).
- Okablowanie skrętkowe w wersji ekranowanej
- **Klasa reakcji: B2ca**

Certyfikaty wydane przez międzynarodowe, renomowane niezależne laboratoria badawcze np. Delta, potwierdzające zgodność okablowania miedzianego z najnowszymi, aktualnymi normami okablowania strukturalnego ISO/IEC 11801:2011 (która zastępuje normy ISO/IEC 11801:2002, ISO/IEC 11801 AMD1:2006, ISO/IEC 11801 AMD2:2010), EN 50173-1:2011, TIA-568-C.2. Należy zapewnić certyfikaty potwierdzające zgodność z normami w zakresie testu całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45).

Okablowanie światłowodowe jednomodowe

Wszystkie produkty muszą być fabrycznie nowe.

Producent okablowania musi objąć zainstalowany system bezpłatną, 25-letnią systemową gwarancją niezawodności, która obejmie tory transmisyjne miedziane i światłowodowe w zakresie łącza Channel (kable instalacyjne, panele 19", złącza, kable krosowe i przyłączeniowe). Gwarancja musi być trójstronną umową podpisaną pomiędzy Użytkownikiem, Wykonawcą okablowania oraz Producentem.

Producent okablowania jest zobligowany do reasekuracji zobowiązań gwarancyjnych Wykonawcy, w przypadku niemożności wywiązania się Wykonawcy z tych zobowiązań. Reasekuracja obejmuje okres, na jaki została udzielona gwarancja.

Warunkiem udzielenia systemowej gwarancji niezawodności jest wykonanie instalacji zgodnie z obowiązującymi normami okablowania strukturalnego oraz zgodnie z zaleceniami producenta. Instalacja musi być wykonana przez Certyfikowanego Instalatora systemu okablowania.

Wymagania ogólne dotyczące systemu okablowania strukturalnego

System okablowania strukturalnego ma zapewnić niezawodną i wydajną warstwę fizyczną sieci teleinformatycznej, która zagwarantuje wystarczający zapas parametrów transmisyjnych dla działania dzisiejszych i przyszłych aplikacji transmisyjnych. W celu spełnienia najwyższych wymogów jakościowych i wydajnościowych należy zapewnić:

- Okablowanie miedziane przewyższające wymagania kategorii 6A (klasy EA).
- Okablowanie skrętkowe w wersji ekranowanej.

Certyfikaty wydane przez międzynarodowe, renomowane niezależne laboratoria badawcze np. Delta, potwierdzające zgodność okablowania miedzianego z najnowszymi, aktualnymi normami okablowania strukturalnego ISO/IEC 11801:2011 (która zastępuje normy ISO/IEC 11801:2002, ISO/IEC 11801 AMD1:2006, ISO/IEC 11801 AMD2:2010), EN 50173-1:2011, TIA-568-C.2. Należy zapewnić certyfikaty potwierdzające zgodność z normami w zakresie testu całego łącza oraz niezależnych komponentów (kabel, panel, złącze RJ45).

Charakteryzuje się dużą giętkością i odpornością na przeciąganie, odporny na promieniowanie UV. Kabel zawiera 12 włókien światłowodowych, wypełniony jest żelem hydrofobowym dla ochrony włókien przed przenikaniem wilgoci. Przeznaczony do instalacji wewnętrznej i zewnętrznej w kanalizacji teletechnicznej. Instalacja może odbywać się metodami mechanicznymi (zaciąganie) oraz pneumatycznymi (wdmuchiwanie).

Kabel zgodny z CPR.

Parametr	Wartość
Tłumienność przy 1310nm	0,35 dB/km
Tłumienność przy 1550nm	0,22 dB/km

Do przyłączenia kabla światłowodowego należy wykorzystać SC/APC. Do urządzeń aktywnych należy wykorzystać wkładki SFP-SC.

Okablowanie poziome

Długość kabla instalacyjnego, pomiędzy gniazdem RJ45 w panelu rozdzielczym a gniazdem przyłączeniowym użytkownika (nie licząc kabli krosowych i przyłączeniowych) nie powinna przekraczać 90m w przypadku urządzeń końcowych typu kamera max. 98m. Celem zapewnienia wysokiej wydajności należy zastosować okablowanie przewyższające wymagania klasy EA (kategorii 6A) wg najnowszych aktualnych standardów okablowania strukturalnego ISO/IEC

11801:2011 (który zastępuje normy ISO/IEC 11801:2002, ISO/IEC 11801 AMD1:2006, ISO/IEC 11801 AMD2:2010), EN 50173-1:2011, TIA-568-C.2. Zagwarantuje to odpowiedni zapas parametrów transmisyjnych dla zapewnienia transmisji danych Ethernet 10Gb/s zgodnie ze standardem IEEE 802.3an. Celem zapewnienia zasilania urządzeniom końcowym, należy zastosować komponenty okablowania strukturalnego zapewniające przesył energii zgodnie ze standardem PoEP (ang. Power over Ethernet Plus) wg IEEE 802.3at o mocy do 30W.

Punkty przyłączeniowe

Gniazda przyłączeniowe użytkowników (Punkty Logiczne – PL) należy zorganizować w postaci 2 lub 4 modułów RJ45 keystone montowanych w adapterze z tworzywa sztucznego o wymiarach 45x45 mm. Ten uniwersalny standard montażowy zapewni organizację gniazd użytkowników w zależności od potrzeb, w formie natynkowej, podtynkowej lub w kasetach podłogowych w oparciu o osprzęt elektroinstalacyjny wielu producentów, również w połączeniu z gniazdami zasilania 230V, celem stworzenia punktów elektryczno-logicznych (tzw. PEL).

Kompaktowy rozmiar pozwalający na zamontowanie dwóch niezależnych modułów RJ45 keystone, również w wersji UTP, w jednym uchwycie montażowym 45 x 45 mm, bez konieczności demontażu standardowej kapsułki ekranującej.

Zasilanie urządzeń końcowych (kamer IP, telefonów IP, punktów dostępowych WiFi itd.) wg najnowszego standardu PoEP.

Moduły RJ45 muszą posiadać pełne ekranowanie 360°, wykonane w postaci pełnej metalowej klatki Faradaya. Metalowa kapsułka ekranująca musi zapewniać pełną szczelność ekranowania od dołu i góry złącza, po bokach i z tyłu oraz z przodu po wpięciu ekranowanego wtyku RJ45. Ponadto należy zachować kontakt ekranu kabla instalacyjnego z ekranem złącza, na pełnym 360° obwodzie kabla, zagwarantuje to bardzo dobre uziemienie ekranu kabla i doskonałą ochronę przed zakłóceniami.

Dodatkowe złącze do uziemienia ekranu kabla instalacyjnego (do podłączenia drutu drenażowego z kabla skrętkowego) celem podwyższenia skuteczności ekranowania kabla. Szeroki zakres temperatury pracy od – 20 °C do + 70 °C.

Instalowanie okablowania strukturalnego

Instalację okablowania strukturalnego należy wykonać z najwyższą starannością z zachowaniem wytycznych znajdujących się w normach okablowania strukturalnego oraz wytycznych producenta okablowania.

- Instalator musi zwrócić szczególną uwagę, by nie naruszyć struktury kabli podczas montażu. Należy przestrzegać bezpiecznych promieni gięcia kabli skrętkowych i światłowodowych, sił naciągu, sił zgniatających oraz przestrzegać zakresu temperatur w czasie instalacji. Dopuszczalne zakresy wymienionych parametrów można znaleźć w specyfikacjach technicznych produktów.
- Kable skrętkowe należy montować w złączach RJ45 zachowując minimalny rozplot par wprowadzanych do złącza.
- Długość skrętkowych kabli instalacyjnych pomiędzy gniazdami RJ45 w panelu rozdzielczym a gniazdami przyłączeniowymi nie może być większa niż 90m.
- Każdy moduł powinien posiadać możliwość rozszycia kabla według schematu T568A i T568B. Zaleca się stosowanie rozszycia wg schematu T568B.
- Wszystkie metalowe części szaf i stelaży dystrybucyjnych muszą zostać uziemione.

- W celu ochrony przed niepożądanym dostępem wszystkie szafy dystrybucyjne oraz pomieszczenia teletechniczne powinny zostać wyposażone w drzwi z zamkami zabezpieczającymi.
- Instalując okablowanie skrętkowe należy zachowywać poniższe bezpieczne odległości od kabli zasilających:

Tabela nr. 1

Typ kabla	Odległość od instalacji zasilającej [mm]		
	Brak przegrody metalicznej	Przegroda metalowa perforowana	Przegroda metalowa pełna
Kable FFTP	10	5	0
Kable UFTP; FUTP	50	25	0
Kabel UUTP	100	50	0

- Tabela obowiązuje dla wiązki 15 obwodów 230V / 20A. W przypadku mniejszej ilości obwodów, odległości proporcjonalnie się zmniejszają.
- Kable 3-fazowe należy traktować, jako 3 kable 1-fazowe.
- Obwody o prądzie większym niż 20A należy traktować, jako proporcjonalna wielokrotność obwodów 20A.
- Powyższe zalecenia obowiązują w przypadku prawidłowego uziemienia ekranów kabli transmisyjnych i metalicznych elementów tras kablowych.

4.3 Rozprowadzenie instalacji

Główne trasy instalacji teletechnicznych zostaną umieszczone na rzutach tras kablowych razem z trasami elektrycznymi. Poniżej opisano sposób prowadzenia okablowania.

Wszystkie nowe kable zasilające instalować zgodnie z rzutami. W przypadku montażu pionowego należy instalować korytka w kolejności od góry:

- korytka instalacji p.poż.
- korytka instalacji teletechnicznej
- korytka instalacji elektrycznej

W przypadku montażu poziomego w kolejności od ściany :

- korytka instalacji p.poż.
- korytka instalacji teletechnicznej
- korytka instalacji elektrycznej

Należy stosować następujące odstępy instalacji teletechnicznej od pozostałych instalacji wg tabeli nr. 1.

W pionach kablowych przewody teletechniczne prowadzić w korytkach kablowych. W pomieszczeniach bez sufitu podwieszanego kable należy układać w rurach osłonowych typu „peszel” podtynkowo. W przestrzeniach, gdzie jest sufit podwieszany kable należy układać w korytkach kablowych i peszlach. Dokładny sposób prowadzenia kabli przedstawiony jest na zamieszczonych rzutach

Kable skrętkowe i światłowodowe okablowania poziomego instalowane pod tynkiem należy układać w rurach osłonowych z tworzywa sztucznego. Nie należy prowadzić kabli telekomunikacyjnych i zasilających w tej samej rurze osłonowej.

Wytyczne montażu tras kablowych

Systemy instalacji elektrycznych będą zapewniać:

- Właściwą ochronę kabli
- trwałość i bezpieczeństwo obsługi
- uniezależnienie od konstrukcji budowlanej
- funkcjonalność i estetykę
- prostotę montażu
- możliwość i łatwość rozbudowy istniejącej instalacji

Wytyczne montażowe dla koryt

Przy wykonywaniu tras kablowych należy pamiętać o zachowaniu następujących zasad:

- rozstaw między podporami tras, powinien być dostosowany do wytrzymałości koryta lub drabiny i nie może powodować przekroczenia maksymalnej obciążalności dopuszczalnej na metr bieżący trasy.
- ostatnia podpora nie może znajdować się dalej niż w odległości 0,5m od końca trasy.
- w przestrzeni między dwiema podporami nie powinno występować więcej niż jedno połączenie śrubowe typu zmiana kierunku trasy lub rozgałęzienia.

Uwagi montażowe

Jeżeli dokonano ucięcia korytka lub drabinki kablowej (przecinarką tarczową lub piłką do metalu) w, każdym przypadku należy:

- Wyrównać krawędzie po cięciu w celu uniknięcia uszkodzenia przewodów.
- Powierzchnie powinny być. - czyste, gładkie, bez zadziorów i wypukłości.
- Zabezpieczyć miejsca w, których wykonano cięcia antykorozyjną farbą cynkową lub spray cynkowy np. FCA ,lub materiałem antykorozyjnym równoważnym technicznie. Powłoka antykorozyjna nie może mieć: pęcherzy, pęknięć i wytrąceń niemetalicznych
- Krawędzie korytek zabezpieczyć taśmą ochronną TO lub TOZ
- Użyte w instrukcji sformułowanie „należy” określa bezwzględną konieczność wykonania danej czynności.

Dokument został opracowany w oparciu o instrukcje zawarte w materiałach producenta, tak, aby wyrób spełniał zasady przydatności do stosowania w budownictwie.

Wykonanie połączeń koryt i drabin kablowych na zasadach opisanych powyżej zapewnia właściwe: wykonanie połączeń wyrównawczych; mocowanie kabli i przewodów izolowanych, sprzętu instalacyjnego możliwość dokonywania zmiany kierunku i płaszczyzn tras, zapobiega uszkodzeniu kabli i przewodów podczas ich układania, oraz w czasie eksploatacji.

Połączenia koryt wykonane w inny sposób niż te, które zostały określone przez producenta łamią zasady przydatności wyrobu do stosowania w budownictwie.

4.4 Pomiary Okablowania Miedzianego

Wszystkie łącza skrętkowe w systemie należy przetestować pod kątem spełniania wymogów klasy EA / kategorii 6A wg ISO 11801 lub EN 50173:

- Należy przeprowadzić pomiary w układzie pomiarowym typu „Channel” (łącznie z kablami krosowymi i kablami przyłączeniowymi). Do pomiaru każdego łącza należy użyć odrębnej pary kabli połączeniowych, która w przyszłości powinna być wykorzystywana w powiązaniu właśnie z tym łączem. W związku z powyższym należy zapewnić pełen zestaw kabli połączeniowych RJ45.
- Pomiary należy wykonać miernikiem o poziomie dokładności, co najmniej „Level IV”. Przykładowe typy mierników: DTX-1800 lub DTX-1200 firmy Fluke Networks.
- Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania.
- Wyniki pomiarów certyfikacyjnych wszystkich łączy muszą być prawidłowe.
- Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.

4.5 Pomiary okablowania światłowodowego

Wszystkie łącza światłowodowe w systemie należy przetestować pod kątem spełniania wymogów norm ISO 11801 lub EN 50173:

- Należy przeprowadzić pomiary dwukierunkowe, w których źródło świetlnego sygnału referencyjnego będzie umieszczone w pierwszym kroku na jednym końcu łącza, a w kolejnym kroku na drugim końcu łącza.
- Łącza wielomodowe (MM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 850 nm i 1300 nm.
- Łącza jednomodowe (SM) należy przetestować w dwóch oknach transmisyjnych, dla długości fali: 1310 nm i 1550 nm.
- Należy wykonać pomiary certyfikacyjne, w których po zmierzeniu rzeczywistych wartości parametrów łącza, miernik automatycznie porówna je z granicznymi wartościami definiowanymi przez aktualne normy okablowania i określi wynik porównania.
- Wyniki pomiarów certyfikacyjnych wszystkich łączy muszą być prawidłowe.
- Pomiary należy wykonać zgodnie z wymaganiami normy PN-EN 50346.
- Wymagany zakres mierzonych parametrów:
 - ☐ Ciągłość łącza.
 - ☐ Długość łącza.
 - ☐ Tłumienie włókien dla dwóch długości fali.

4.6 Dane techniczne urządzeń aktywnych

Switch 48xRJ45 2xSFP

- Gigabitowe Porty: 48 Gigabitowe Porty RJ45 i 2 Gigabitowe Sloty SFP zapewniają wysokie prędkości połączeń.
- Możliwość korzystania z Omada SDN: Platforma zapewnia dostęp do bezobsługowej konfiguracji ZTP*, centralnego zarządzania w chmurze oraz inteligentnego monitoringu.
- Scentralizowane zarządzanie: dostęp z chmury oraz łatwej w użytkowaniu aplikacji Omada.

- Statyczny Routing: Umożliwia kierowanie ruchem sieciowych dla efektywnego wykorzystania zasobów sieciowych
- Silne strategie zabezpieczeń: IP-MAC-Port Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X, Radius Authentication i wiele innych.
- Optymalizacja aplikacji Głosowych i Wideo: L2/L3/L4 QoS i IGMP snooping.
- Zarządzanie: Web, CLI (Port konsolowy, Telnet, SSH), SNMP, RMON i Dual Image dają duże możliwości zarządzania

Switch 24xRJ45 2xSFP

- Gigabitowe Porty: 24 Gigabitowe Porty RJ45 i 4 Gigabitowe Sloty SFP zapewniają wysokie prędkości połączeń.
- Możliwość korzystania z Omada SDN: Platforma zapewnia dostęp do bezobsługowej konfiguracji ZTP*, centralnego zarządzania w chmurze oraz inteligentnego monitoringu.
- Scentralizowane zarządzanie: dostęp z chmury oraz łatwej w użytkowaniu aplikacji Omada.
- Statyczny Routing: Umożliwia kierowanie ruchem sieciowych dla efektywnego wykorzystania zasobów sieciowych
- Silne strategie zabezpieczeń: IP-MAC-Port Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X, Radius Authentication i wiele innych.
- Optymalizacja aplikacji Głosowych i Wideo: L2/L3/L4 QoS i IGMP snooping.
- Zarządzanie: Web, CLI (Port konsolowy, Telnet, SSH), SNMP, RMON i Dual Image dają duże możliwości zarządzania

Switch 16xRJ45 2xSFP

- Gigabitowe porty: 16 gigabitowych portów RJ45 i 2 gigabitowe sloty SFP przekładają się na stabilne połączenia o dużych prędkościach.
- Działanie zintegrowane z platformą Omada SDN: Bezobsługowa konfiguracja ZTP*, centralne zarządzanie w chmurze i inteligentne monitorowanie.
- Centralne zarządzanie: Dostęp z poziomu chmury i aplikacja Omada to wygoda zarządzania.
- Routing statyczny: Sterowanie ruchem wewnętrznym daje możliwość efektywniejszego wykorzystania zasobów sieciowych.
- Niezawodne zabezpieczenia: Wiązanie adresów IP, MAC i portów, ACL, Port Security, ochrona przed atakami DoS, Storm Control, DHCP Snooping, 802.1X, uwierzytelnianie poprzez serwer Radius i wiele więcej.
- Optymalizacja transmisji głosu i wideo: QoS L2/L3/L4 i IGMP Snooping.
- Samodzielne zarządzanie: Witryna, CLI (port konsolowy, Telnet, SSH), SNMP, RMON i Dual Image dają duże możliwości zarządzania.

CECHY SPRZĘTOWE	
Porty	• 16 portów RJ45 10/100/1000 Mb/s
	• 2 gigabitowe sloty SFP
Bezwentylatorowy	Tak
Zasilanie	100-240 V AC~50/60 Hz

Wymiary (S x G x W)	440 × 180 × 44 mm
	(17,3 × 7,1 × 1,7)
Montaż	Możliwość montażu w szafie rack
Maks. zużycie energii	12,3 W
Ilość generowanego ciepła	41,97 BTU/hr
WYDAJNOŚĆ	
Wydajność przełączania	36 Gb/s
Szybkość przekierowań pakietów	26,8 Mp/s
Tablica adresów MAC	8K
Ramki jumbo	9 KB

Switch PoE 12xRJ45 2xSFP

Gigabitowy Przełącznik Smart JetStream, 12 portów PoE+, 2 Sloty SFP

- 150 W zasilania PoE: 12 portów PoE+ zgodnych ze standardem 802.3at/af i łącznym zasilaniem do 150W*.
- Gigabitowe Porty: 8 Gigabitowych Portów PoE+ i 2 Gigabitowe Sloty SFP zapewniają wysokie prędkości połączeń.
- Możliwość korzystania z Omada SDN: Platforma zapewnia dostęp do bezobsługowej konfiguracji ZTP**, centralnego zarządzania w chmurze oraz inteligentnego monitoringu.
- Scentralizowane zarządzanie: Zarządzanie jest niezwykle wygodne dzięki dostępowi z chmury oraz łatwej w użytkowaniu aplikacji Omada.
- Silne strategie zabezpieczeń: IP-MAC-Port Binding, ACL, Port Security, DoS Defend, Storm control, DHCP Snooping, 802.1X, Radius Authentication i wiele innych.
- Optymalizacja aplikacji Głosowych i Wideo: L2/L3/L4 QoS i IGMP snooping.

Switch PoE 24xRJ45 2xSFP

- 24 porty PoE+ zgodne ze standardami 802.3at/af, maksymalna moc całkowita podłączonych urządzeń do 192W
- Funkcja routingu statycznego warstwy 2+ pozwala na zwiększenie wydajności sieci
- Rozbudowane funkcje zabezpieczające ruch sieciowy, w tym obsługa VLAN 802.1Q, Port Security oraz Storm control umożliwiają skuteczne zabezpieczenie sieci lokalnej.
- Możliwość zoptymalizowania transmisji głosowych oraz wideo dzięki funkcjom QoS (L2/L3/L4) oraz IGMP snooping.
- Obsługa IPv6 z możliwością podwójnego stosu IPv4/IPv6, MLD snooping oraz IPv6 neighbor discovery

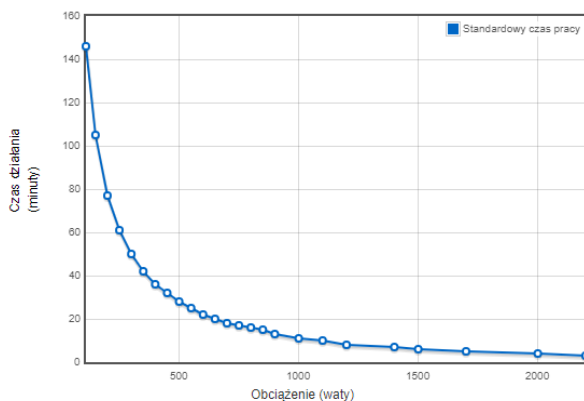
- Zarządzanie z wiersza poleceń oraz poprzez przeglądarkę internetową, obsługa SNMP, RMON oraz Dual Image umożliwiając wygodne zarządzanie urządzeniem.

CECHY SPRZĘTOWE	
Standardy i protokoły	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.3az, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p, IEEE 802.1x
Porty	24 porty RJ45 10/100/1000Mb/s
	(Auto negocjacja/Auto MDI/MDIX)
	2 gigabitowe sloty SFP
Okablowanie sieciowe	10BASE-T: Kabel UTP kat. 3, 4 lub 5 (do 100m)
	100BASE-TX/1000Base-T: Kabel UTP kat. 5, 5e lub wyższej (do 100m)
	1000BASE-X: MMF, SMF
Bezwentylatorowy	Nie - 2 wentylatory
Zasilanie	100~240VAC, 50/60Hz
Porty PoE+ (RJ45)	Zgodność ze standardami:802.3at/af
	Liczba portów PoE+: 24
	Maksymalna łączna moc podłączonych urządzeń: 192W
Wymiary (S x G x W)	440 * 220 * 44 mm (17,3 * 8,7 * 1,73 cala)
Montaż	Do montażu w szafie
Maks. zużycie energii	30,77W (110V/60Hz bez podłączonych PD)
	235,8W (110V/60Hz z podłączonymi urządzeniami PD 192W)
Ilość generowanego ciepła	104,99 BTU/h (bez podłączonych PD)
	804,55 BTU/h (z podłączonymi urządzeniami PD 192W)
WYDAJNOŚĆ	
Przepustowość	56Gb/s

Szybkość przekierowań pakietów	41,7Mp/s
Tablica adresów MAC	8K
Ramki jumbo	9KB

UPS 2200VA

DLUGOŚĆ/GŁĘBOKOŚĆ PRODUKTU	483 mm	ZAKRES NAPIĘCIA WYJŚCIOWEGO	230 V (+6%-10%)
WYSOKOŚĆ PRODUKTU	129 mm	TOPOLOGIA	Technologia line-interactive
SZEROKOŚĆ PRODUKTU	438 mm	CZAS PRACY PRZY POŁOWICZNYM OBCIĄŻENIU	10 min
MAŚA PRODUKTU	27.5 kg	NAPIĘCIE ZNAMIONOWE WEJŚCIOWE	Domyślne 230 V (200/208/220/230/240 V)
ZGODNOŚĆ/ZGODNOŚCI	IEC/EN 62040-1 IEC/EN 62040-2 IEC/EN 62040-3 Zgodny z wymogami RoHS REACH UL 1778 CSA 22.2	ZAKRES CZĘSTOTLIWOŚCI WEJŚCIOWYCH	47-70 Hz (system 50 Hz), 56,5-70 Hz (system 60 Hz), 40 Hz w trybie niskiej częstotliwości
CERTYFIKAT(Y)	CE cTUVus EAC Cm UKCA ULtr ENERGY STAR certified	NAPIĘCIE WEJŚCIOWE — MAKS.	294 V
CZĘSTOTL. WΤΩRNA – MAKS.	60 Hz	RODZAJ NAPIĘCIA	AC
KSZTAŁT FALI NA WYJŚCIU	Fala sinusoidalna	FAZA (WYJŚCIE)	1
MAKSYMALNA LICZBA AKUMULATORÓW	4	POZIOM HAŁASU	Mniej niż 40 dB w odległości 1 m
MOC	2200 W	TYP ZASILANIA	1
WYJŚCIOWY WSPÓŁCZYNNIK MOCY	1	WYKRES CZASU PODTRZYMYWANIA DZIAŁANIA	Patrz wykres czasu podtrzymywania działania
WSPÓŁCZYNNIK KSZTAŁTU	Szcza rack/wieża	INTERFEJS UŻYTKOWNIKA	Wielojęzyczny, graficzny wyświetlacz LCD
ZAWIERA KARTĘ SIECIOWĄ	Nie	LICZBA AKUMULATORÓW	6
ZŁĄCZE WEJŚCIOWE	C20	ROZMIAR SZAFY RACK	3U
NAPIĘCIE WEJŚCIOWE — MIN.	150 V	ZAKRES NAPIĘCIA	230 V
NAPIĘCIE WYJŚCIOWE — MAKS.	240 V	DLUGOŚĆ PRZEWODU WEJŚCIOWEGO	1.8 m
CZĘSTOTL. WΤΩRNA – MIN.	50 Hz	ZAKRES TEMPERATURY	Od 0° do 40° C (od 32°F do 104°F), zalecana maks. temperatura 25° C (77°F)
KOMPATYBILNOŚĆ OPROGRAMOWANIA	Oprogramowanie: Intelligent Power Manager, Intelligent Power Protector	LĄCZNOŚĆ	Port USB (kompatybilny z HID) Port szeregowy (RS232) Mini-terminal zacisków do zdalnego włączania/wyłączania i zdalnego wyłączania Mini-terminal zacisków do przekablała wyjściowego Słuki bezpieczeństwa (3 wyjścia, 1 wejście, transceptor, DB9)
WYMIANA AKUMULATORÓW	Możliwość wymiany przez użytkownika	WILGOTNOŚĆ WZGLĘDNA	0-90%, bez kondensacji
RODZAJ AKUMULATORA	Kwasowo-ołowiowy, bezobsługowy (wymienny)	ZESTAW DO MONTAŻU W SZAFACH RACK	Tak
SPRAWNOŚĆ	98	LICZBA WYJŚĆ PC (SCHUKO)	0
LICZBA WYJŚĆ Z POŁĄCZENIAMI KABLOWYMI	0	CZĘSTOTLIWOŚĆ NAPIĘCIA WYJŚCIOWEGO	50/60 Hz
LICZBA POŁĄCZEŃ WYJŚCIOWYCH, NORMA FRANCUSKA (TYP E)	0	RODZAJ INTERFEJSU	Inny
Cechy specjalne	System automatycznej regulacji napięcia (AVR) Energoszczędność, redukcja kosztów energii i chłodzenia Zapewnia sygnał wyjściowy w postaci czystej sinusoidy Dzięki współczynnikowi mocy równemu 1 (0.99) zapewnia największą moc czynną (W), co pozwala obsługiwać urządzenia Wyświetlacz LCD prezentujący status i pomiary w czasie rzeczywistym Długi czas podtrzymania z maksymalnie 4 opcjonalnymi modułami EBM Miejsce załadunku energii (do zasilaczonych grup urządzeń) Wszelchotrony produkt do montażu w szafach lub wieżach 1 gniazdo na opcjonalną kartę komunikacyjną (karta sieciowa, karta przekablniowa lub karta sieciowa i do zastosowań przemysłowych) Kompatybilność ze środowiskami wirtualnymi (VMware, Hyper-V, Citrix Xen, Redhat) 1 port USB + 1 port szeregowy	CZĘSTOTLIWOŚĆ PODSTAWOWA - MIN.	47 Hz
RODZAJ BUDOWY	urządzenie 482,6 mm (19 cali)	PARAMETRY ZNAMIONOWE AKUMULATORA	12 V / 7 Ah
NAPIĘCIE WYJŚCIOWE — MIN.	200 V	TYP	UPS
KOLOR	Czarny/srebrny	NAPIĘCIE ZNAMIONOWE WYJŚCIOWE	Domyślne 230 V (200/208/220/230/240 V)
ZWIĘKSZONE MOŻLIWOŚCI AKUMULATORA	Tak	GNIAZDA ROZSZERZEŃ	Jedno gniazdo na opcjonalną kartę komunikacyjną
		ZAKRES NAPIĘCIA WEJŚCIOWEGO	160-294 V (regulowane do 150 V-294 V)
		CZĘSTOTLIWOŚĆ ZNAMIONOWA	50-60 Hz
		CZĘSTOTLIWOŚĆ PODSTAWOWA - MAKS.	70 Hz
		WYSOKOŚĆ N.P.M.	3000 m



4.7 Instalacja CCTV

System monitoringu obejmuje wejścia do budynku, komunikację, kancelarię tajną. Projektuje się system oparty o kamery IP. Serwer systemu CCTV ma umożliwiać archiwizację nagrań na minimum 30 dni jak również analitykę obrazu. Rzut rozmieszczenia kamer i schemat instalacji załączony jest na rzutach.

Kamery należy podłączyć do nowych punktów dystrybucyjnych jak również pod wideo rejestratory. W przypadku braku wspierania dedykowanego protokołu dopuszcza się możliwość stosowanie protokołów generycznych takich jak Onvif oraz PSIA w celu połączenia urządzenia z platformą. Wymagane jest obsługiwanie wbudowanych w kamerę algorytmów badania, jakości obrazu kamery w celu ułatwienia zarządzania wielokamerowymi poprzez automatyczne poinformowanie operatora, administratora o utracie jakości obrazu.

W zespole pomieszczeń kancelarii tajnej zostanie wykonana odrębna instalacja monitoringu z rejestratorem umieszczonym w szafie LPD1, gdzie wyodrębniony zapis obrazu z kamery przed drzwiami KT, przechowywany przez min 30 dni, - zarządza wyłącznie lokalny administrator systemu.

Założenia funkcjonalne dla poszczególnych komponentów systemu CCTV IP:

4.8 Opis zastosowanych kamer

W projekcie zostały przewidziane kamery zewnętrzne z detekcją ruchu i perymetrią, Rozdzielczość kamer 8 MP.

Kamery kopułkowe wandaloodporne PTRZ

Opis funkcjonalny:

Do dozoru przestrzeni wewnętrznych oraz zewnętrznych planuje się wykorzystanie kamer kopułkowych wandaloodpornych, o rozdzielczości 8 Mpx (4K UHD). Kamery posiadały będą przetworniki pracujące w technologii wysokiej czułości gwarantując do 0,0072 luxa w trybie nocnym.

Kamera daje możliwość w pełni zdalnej regulacji położenia obiektywu w trzech osiach, dzięki czemu możliwe jest dokładne dopasowanie obserwowanej sceny w dowolnym momencie, już po zamontowaniu kamery i bez konieczności demontażu kopułki. Ponadto, zintegrowany obiektyw umożliwia regulację zoom'u i ostrości.

Z racji dużej liczby kamer w systemie security, celem zachowania efektywności systemu bez znaczącego zwiększenia liczby operatorów przyjmuje się aktywne wykorzystanie mechanizmów zaawansowanej analizy obrazów dla kamer CCTV. Tym samym wszystkie kamery w systemie będą fabrycznie wyposażone w funkcje inteligentnej analizy obrazu – nie wymaga to zakupu i uruchamiania dodatkowych licencji. Analiza obrazu odbywa się bezpośrednio w kamerze, dzięki czemu zapewniona jest najwyższa skuteczność (praca na nieskompresowanym obrazie) oraz skalowalność. Zakłada się wykorzystanie co najmniej następujących algorytmów analizy:

- Wykrywanie porzucenia przedmiotów
- Wejście w zastrzeżoną strefę
- Zliczanie obiektów

- Nienaturalne szwędanie się osób w wyznaczonych obszarach

W celu znacznie skuteczniejszego wykorzystania funkcji inteligentnej analizy obrazu, kamera będzie w stanie automatycznie sklasyfikować rozpoznany obiekt (jako człowieka, rowerzystę, czy samochód). Rodzaj obiektu będzie wskazany na obrazie poprzez wyświetlanie odpowiedniej ikonki, obok dokładnego obrysu obiektu.

Kamera posiada funkcjonalność uczenia maszynowego, dzięki czemu funkcje inteligentnej analizy obrazu mogą reagować na dowolny, zdefiniowany przez użytkownika kształt w obserwowanej scenie. W efekcie, możliwe jest skuteczne wykrywanie różnego rodzaju obiektów (np. samochodów osobowych, ławek czy wózków) lub stanów (np. otwarcie szlabanu). Możliwa jest również detekcja obiektów nieruchomych, dzięki czemu kamera może być zastosowana do gromadzenia dodatkowych danych statystycznych, jak np. zajętości miejsc parkingowych.

Kamera jest w stanie w sposób automatyczny zmieniać parametry wszystkich strumieni wizyjnych, w zależności od określonego harmonogramu lub wystąpienia stanu alarmowego. Ponadto, kamera umożliwia zapisywanie skryptów, w celu tworzenia odpowiednich zależności logicznych i rozbudowanych reakcji na alarmy, bezpośrednio w kamerze.

Celem zwiększenia efektywności i skrócenia czasu przeszukiwania nagrań przez operatorów, algorytmy inteligentnej analizy obrazów wykorzystywane będą również do analizy wstecznej. Przeszukiwanie nagrań odbywać się będzie niezależnie od wcześniej skonfigurowanych alarmów w kamerze – w zależności od aktualnych potrzeb operatora. Na podstawie metadanych zbieranych w systemie analityki, operator będzie w stanie szybko przeszukać zapisy pod kątem zdarzeń takich jak:

- Pojawienia się w scenie obiektów sklasyfikowanych jako człowiek lub samochód osobowy;
- Określenia kierunku poruszania się osoby lub pojazdu;
- Określenia koloru ubioru osoby lub koloru pojazdu;

Istotną kwestią będzie także cyberbezpieczeństwo całego układu sieciowego i wszystkich systemów security bazujących na nim. Zakłada się szyfrowaną komunikację pomiędzy kamerami, serwerem zarządzającym, stacjami operatorskimi i systemem zapisu, przy wykorzystaniu algorytmów szyfrujących AES z kluczem 256 bit.

Kamera daje możliwość obsługi dwóch kart SD o pojemności do 2 TB. W przypadku zastosowania kart w wykonaniu przemysłowym kamera może monitorować aktualny stan karty i automatycznie alarmować, w przypadku przekroczenia określonego limitu jej żywotności.

Kamera daje możliwość zapisania danych geolokacyjnych – na temat dokładnych współrzędnych jej położenia – co przy zastosowaniu odpowiedniego oprogramowania umożliwia dokładne umiejscowienie kamery na mapie i oznaczenie na mapie wykrytych obiektów.

Kamera daje możliwość skonfigurowania do 8 masek prywatności. Aby zapewnić odpowiednią czytelność obrazu dostępne są do wyboru 3 kolory masek, w tym maska zlewająca się z kolorem tła.

Wymagania techniczne:

Parametr	Wymagania minimalne
Budowa	Kamera kopułkowa wandaloodporna
Rozdzielczość	3840 x 2160 p30
Przetwornik	CMOS 1/1,8"
Czułość	Nie gorsza niż 0,041 lux w trybie dziennym i 0,0072 lux w trybie nocnym dla 1/25, F1.5 (zgodnie z IEC 62676 Część 5)
Zakres dynamiki	120 dB
Kompresja	H.264; H.265; M- JPEG
Obszary ROI	Do 8 obszarów z niezależnymi ustawieniami jakości kodowania
Stosunek sygnał/szum	>55 dB
Migawka	Tryby migawki: automatyczna, wybierana ręcznie.
Regulacja położenia obiektywu	W pełni zdalna, w 3 osiach, za pośrednictwem przeglądarki sieciowej lub dodatkowej aplikacji
Zakres zdalnej regulacji obiektywu	Obrót horyzontalny: 0° do +361° Pochylenie: -3.5° do +89°

	Obrót wokół osi obiektywu: -95° do +95°
Obiektyw	Zintegrowany 3,9 - 10 mm ze zdalną regulacją położenia oraz zdalną regulacją zoom i autofocusem
Obsługiwane protokoły	IPv4, IPv6, UDP, TCP, HTTP, HTTPS, RTP/RTCP, IGMP V2/V3, ICMP, ICMPv6, RTSP, FTP, ARP, DHCP, APIPA (Auto-IP, link local address), NTP (SNTP), SNMP (V1, V3, MIB-II), 802.1x, DNS, DNSv6, DDNS, SMTP, iSCSI, UPnP (SSDP), DiffServ (QoS), LLDP, SOAP, Dropbox™, CHAP, digest authentication
Bezpieczeństwo danych	Wsparcie uwierzytelnienia poprzez protokół EAP-TLS 1.2 także z możliwością wgrania certyfikatu w zakresie infrastruktury klucza publicznego do szyfrowania cyfrowego dostarczonego przez producenta kamery, tworzonego przez użytkownika oraz certyfikowane rozwiązania firm 3-ch
	Wsparcie szyfrowania na poziomie sprzętowym tj fabrycznie zabudowany moduł TPM (Trusted Platform Module), który wykorzystuje klucz kryptograficzny do ochrony wszystkich zarejestrowanych danych
Autentykacja wideo	Znak wodny, SHA-1, SHA-256
Łącze sieciowe	RJ-45 100 Base-TX Ethernet
Strumienie wideo	Możliwość generowania 4 strumieni wideo
Inteligentna analiza obrazów	Wbudowana w kamerę z możliwością równoległej analizy do 8 reguł alarmowych
	Analizowane algorytmy: <ul style="list-style-type: none"> • wykrycie obiektu • przekroczenie linii • kierunkowość ruchu • porzucenie obiektu • zmiana stanu obiektu • zliczanie – przekroczenie linii • zliczanie obiektów w określonych strefach
	Zaawansowane funkcje w zakresie kalibracji i monitorowania obiektu takie jak np. ustalone proporcje obiektu, kolor obiektu oraz kierunek i prędkość jego przemieszczania
	Możliwość prezentowania statystyki dla wybranego pola lub obiektu z możliwością odczytu rzeczywistych wartości takich jak prędkości obiektu, jego proporcje i kolor czy kierunek jego poruszania
	Możliwość analizy materiału zarejestrowanego na podstawie metadanych
	Funkcja uczenia maszynowego, umożliwiająca samodzielne tworzenie dowolnych detektorów na podstawie obserwowanych przez kamerę kształtów
Zapis lokalny	Wbudowane 2 sloty kart SD (obsługa kart do 2 TB)
Pre-alarm	5s (w kamerze)
Zgodność	ONVIF Profile S; Profile G; Profile T
Wejście alarmowe	2
Wyjście przekaźnikowe	1
Wejście audio	1
Wyjście audio	1
Maski prywatności	8
Temperatura pracy	-50 - +60 °C
Stopień ochrony	IP66
Wandaloodporność	IK10+
Zasilanie	12 VDC lub PoE
Gwarancja	3 lata

4.9 Serwer zarządzania i rejestracji

Zastosowane w projekcie rejestratory są uniwersalnymi rozwiązaniami do rejestrowania, wyświetlania oraz zarządzania obrazami.

Do rejestratora w szafie GPD2 przewidziano 4 dysków po 18TB (przystosowane do pracy ciągłej). Rejestrację z kamer w czasie min. 30 dni.

Dodatkowo należy zainstalować stację roboczą w pomieszczeniu portiera lub w każdej innej lokalizacji gdzie jest gniazdko RJ45 i połączyć z monitorem.

Bilans doboru dysków HDD dla rejestratora CCTV1:

Cameras Bandwidth	Storage Devices Bandwidth	Gross Storage Needed	Gross Storage Added	RAID Version	Retention Time
138.59 Mbps	400 Mbps	53.12 TB	72 TB	RAID5	30 days

Dla zapisu 32 kamer 30 dni z prędkością 15fps z rozdzielczością 8Mpx w trybie 24h/dobę, przy kompresji H.264 - 53,2TB

Należy zrealizować na (4x18TB)



Serwer rejestracji

1. Do rejestracji obrazu z kamer w systemie planuje się wykorzystanie dedykowanej macierzy dyskowej, służącej jako przestrzeń dyskowa do zapisu.
2. Urządzenie jest przeznaczone do bezpośredniego montażu w szafie rack.
3. Serwer rejestrujący jest dostarczony od producenta w formie prekonfigurowanej, w formie gotowej do podłączenia do oprogramowania zarządzającego.
4. Pojedynczy serwer umożliwia podłączenie, zarządzanie i rejestrację do 64 kamer (kanałów wideo) w systemie.
5. Serwer jest wyposażony w dyski SATA-3 do rejestracji, do których zapewniony jest dostęp od frontu urządzenia, umożliwiając łatwą wymianę dysków.
6. Serwer posiada wbudowany transkoder, umożliwiający wykorzystanie technologii transkodowania dynamicznego, dopasowującego parametry strumienia wizyjnego, przekazywanego do aplikacji klienckich, do aktualnych możliwości łącza.
7. Serwer rejestrujący wspiera technologie SNMP, zdalnego pulpitu czy monitorowania http elementów sprzętowych i aplikacji zarządzającej.
8. Serwer powinien być objęty co najmniej 5-letnią gwarancją producenta.
9. Podstawowe parametry techniczne serwera zestawiono w poniższej tabeli:

Bilans doboru dysków HDD dla rejestratora CCTV2:

Kalkulator wymaganej pojemności dysku w rejestratorze

Metoda kompresji:	<input type="radio"/> H.265+ <input type="radio"/> H.265 <input checked="" type="radio"/> H.264 (Najczęściej stosowana) <input type="radio"/> MPEG-4 <input type="radio"/> MPEG-2 <input type="radio"/> MJPEG
Rozdzielczość zapisu:	<input type="radio"/> QCIF (176x120) <input type="radio"/> 1 Megapixel (1280x720) <input type="radio"/> 5 Megapixel (2592x1944) <input type="radio"/> CIF (352x240) <input type="radio"/> 2 Megapixel (1920x1080) <input checked="" type="radio"/> 8 Megapixel (3840x2160) <input type="radio"/> 4CIF (704x480) <input type="radio"/> 3 Megapixel (2048x1536) <input type="radio"/> 12 Megapixel (4000x3000) <input type="radio"/> D1 (720x576) <input type="radio"/> 4 Megapixel (2560x1440)
Jakość zapisu:	<input checked="" type="radio"/> Wysoka <input type="radio"/> Średnie <input type="radio"/> Niska
Rozmiar klatki:	81 KB
Ilość kamer:	1
Ilość klatek na sekundę z każdej kamery:	16 klatek/sekundę
Ilość godzin zapisu na dobę:	24 h/doba
Wymagany czas archiwizacji:	30 dni
Strumień zapisu:	15.55 Mbps → na 1 kamerę 15.55 Mbps
Minimalna pojemność dysku:	10.08 TB

Przydatne informacje:

- W większości przypadków wystarczy zapis z prędkością 6 klatek/sekundę (FPS)
- 10 klatek/sekundę (FPS) sprawia wrażenie płynnego ruchu

Dobrano 4x4TB

4.10 Stacja robocza:

Podgląd obrazu wideo z kamer prezentowany będzie na dedykowanej stacji klienckiej typu PC wielomonitorowej (2 monitory, 32" każdy)

W projekcie zastosowano 2 stacje robocze (pom. 0.04 stałego dyżuru i kancelaria tajna) z 2 monitorami 32" umożliwiającymi monitoring. Stacja robocza w kancelarii tajnej zostanie podłączona z szafą LPD1, stacja robocza w pom 0.04 z serwerem BMS poprzez szafę GPD2.

Ilość monitorów: 4szt.

5 Instalacja Kontroli Dostępu

W pomieszczeniach objętych kontrolą dostępu została zastosowana Klasa rozpoznania 2 (rozpoznanie bazujące na danych zawartych na identyfikatorze) i klasa dostępu A (klasa nie wymaga stosowania siatki czasu i rejestracji transakcji uzyskiwania dostępu).

W kancelarii tajnej zastosowano klasę rozpoznania 3 (Rozpoznanie bazuje na powiązaniu odczytu identyfikatora i biometriki z wprowadzeniem informacji zapamiętanych) jak również klasę dostępu B (wykorzystanie funkcji siatki czasu oraz rejestracji zdarzeń). Kontrola dostępu dwustronna.

W pomieszczeniu serwerowni zastosowano klasę rozpoznania 3 (Rozpoznanie bazuje na powiązaniu odczytu identyfikatora i biometriki z wprowadzeniem informacji zapamiętanych) jak również klasę dostępu B (wykorzystanie funkcji siatki czasu oraz rejestracji zdarzeń). Kontrola dostępu dwustronna.

Zgodnie z wymaganiami projektuje się instalację Systemu Kontroli Dostępu dla następujących obszarów/przejęć:

- wydzielonych pomieszczeń służbowych i biurowych
- pomieszczenia techniczne lub przejścia do nich.
- pomieszczenia porządkowe

Część przejść do pomieszczeń będą przejściami dwustronnymi tzn. wejście i wyjście do obszaru chronionego odbywa się za pomocą karty. Dodatkowo zainstalowany zostanie awaryjny przycisk wyjścia.

Wszystkie przejścia będą posiadać:

- kontrolę ich stanu (otwarte/zamknięte);
- urządzenia blokujące przejście – odpowiednie dla każdego rodzaju zamknięć;
- urządzenia samozamykające przejście – odpowiednie dla każdego rodzaju zamknięć;

Każde z projektowanych przejść wyposażone będzie w następujące urządzenia:

- czytnik kart zbliżeniowych od strony wejścia i wyjścia lub tylko wejścia
- czujkę magnetyczną monitorującą stan otwarcia drzwi
- elektrozamek
- samozamykacz drzwiowy - opcja

Do obsługi powyższych urządzeń danego przejścia będzie zainstalowany kontroler dostępu, który będzie realizował funkcje w zakresie kontroli dostępu.

Pomieszczenia podlegające ochronie KD będą otwierane automatycznie w przypadku pożaru poprzez system SSP (według schematu SSP i matrycyysterowań).

W przypadku kontroli dostępu dwustronnej został dołożony dodatkowy awaryjny przycisk wyjścia.

Generalnie projektuje się system kontroli dostępu jednostronny.

Do głównych i bocznych wejść do budynku oraz do niektórych pomieszczeń o szczególnym znaczeniu będzie wykonana dwustronna kontrola dostępu.

System kontroli dostępu będzie zintegrowany z systemem alarmowym, jak również zostanie wykonana wizualizacja zintegrowanych systemów.

Czytniki

W systemie należy zastosować adresowalne czytniki umożliwiające dwukierunkową komunikację z kontrolerem. Dane odczytane z karty RFID jak również sygnały wymieniane pomiędzy czytnikiem oraz kontrolerem (np. sterowanie diodami, sygnalizacja sabotażu) powinny być przesyłane po protokole komunikacyjnym.

Komunikacja z czytnikami powinna być ciągle monitorowana. W przypadku utraty łączności z czytnikiem odpowiedni sygnał alarmowy powinien zostać wysłany do centralnego oprogramowania zarządzającego-monitorującego. Dodatkowo czytniki powinny być zabezpieczone antysabotażowo i wysyłać odpowiedni sygnał alarmowy w przypadku demontażu czytnika.

System powinien gwarantować maksymalną uniwersalność w przypadku przyszłych rozbudów dlatego zastosowane czytniki oraz kontrolery przejść powinny wykorzystywać do komunikacji ustandaryzowane protokoły (nie produkcyjne rozwiązania) takie jak OSDP, które umożliwiają zastosowanie czytników wielu producentów.

Należy zastosować czytniki o zwiększonej odpornością na działanie czynników zewnętrznych (min. IP65). Czytniki wyposażone w klawiaturę powinny mieć podświetlane przyciski.

Kontrolery sterujące KD

System kontroli dostępu powinien mieć strukturę opartą o autonomiczne kontrolery sieciowe podłączonych do serwera zarządzającego z wykorzystaniem protokołu TCP/IP.

Każdy z modułów bezpośrednio sterujący przejściem (do który podłączone są czytniki RFID) powinien być wyposażony w port Ethernet. Umożliwi to wykorzystanie infrastruktury sieciowej obiektu.

Dla zapewnienia niezawodnej pracy systemu, nawet w przypadku awarii sieci, kontrolery powinny cechować się autonomicznym działaniem. W przypadku utraty komunikacji kontrolera z pozostałą częścią systemu kontroler do którego bezpośrednio podłączone są czytniki oraz elementy peryferyjne przejścia powinien umożliwiać obsługę wszystkich kart zdefiniowanych w systemie oraz zapis zdarzeń w wewnętrznej pamięci. Zdarzenia powinny zostać automatycznie przesyłane do serwera po przywróceniu komunikacji tak aby mieć dostęp do zdarzeń zarejestrowanych w chwili awarii łączności lub przy próbie sabotażu systemu.

Autonomiczny kontroler sieciowy powinien obsługiwać ograniczoną ilość przejść tak aby awaria pojedynczego kontrolera powodowała wyłącznie z działania maksymalnie 8 przejść kontroli dostępu.

Karty RFID – Mifare DESFire

W systemie należy zastosować bezpieczną technologię kart RFID, w której do identyfikacji wykorzystywane są zaszyfrowane dane zapisane na karcie. Nieakceptowalne jest wykorzystywanie numerów seryjnych kart CSN/UID do identyfikacji w systemie.

Projektowane czytniki kontroli dostępu powinny umożliwiać odczyt zaszyfrowanych danych z kart RFID z możliwością wyłączenia odczytu numerów seryjnych kart (CSN/UID) dla zwiększenia bezpieczeństwa obiektu.

Zastosowane zabezpieczenia danych w karcie powinny uniemożliwić kopiowanie oraz nieuprawniony odczyt danych z kart. Należy zastosować nieskompromitowaną technologię (np. odczyt aplikacji z kart Mifare DESFire z szyfrowaniem).

OPROGRAMOWANIE ZARZĄDZAJĄCE I INTEGRUJĄCE

W ramach projektu przewiduje się instalację systemu integrującego wszystkie podsystemy bezpieczeństwa w obiekcie. Interfejs graficzny operatora (GUI), jak również aplikacja do konfiguracji muszą być dostępne w języku polskim.

System ten ma mieć możliwość sterowania/nadzorowania:

- systemu kontroli dostępu,
- systemu sygnalizacji włamania i napadu,
- systemu sygnalizacji pożaru – tylko wizualizacja,
- systemu telewizji dozorowej,
- systemów trzecich, jak np. automatyki przemysłowej czy budynkowej.

System charakteryzuje się budową modułową – do integracji wybranego podsystemu i urządzeń wchodzących w jego skład jest wymagany jedynie określony silnik programu. Rozbudowa systemu i podłączenie kolejnych elementów jest możliwa w dowolnym momencie.

System integrujący posiada otwartą architekturę i wsparcie dla przemysłowych standardów baz danych, sieci, rysunków, kamer wideo, takich, jak:

- OPC,
- AutoCAD,
- HTML 5,
- ASPX,
- Jscript
- SQL

Podstawowym standardem integracji jest otwarty protokół OPC, dzięki czemu możliwe jest podłączenie dowolnego podsystemu, różnych producentów. Oprogramowanie wspiera również najnowszy standard OPC UA, umożliwiający m.in. integrację z systemami automatyki po standardowych protokołach przemysłowych.

Stany poszczególnych elementów podsystemów będą wizualizowane na mapach wektorowych (np. AutoCAD), co jest rozwiązaniem optymalnym dla pracy z większymi mapami, gdy konieczne jest zbliżanie/oddalanie widoku. Mapa, oparta o rysunek wektorowy, umożliwia stworzenie logicznego podziału na obszary i nadanie im niezależnych nazw.

System daje możliwość włączania/wyłączania określonych warstw wyświetlanej mapy (np. warstw z elementami danego podsystemu, przebiegu tras kablowych, itp.) przez operatora, w dowolnym momencie pracy. Włączanie/wyłączanie określonych warstw wyświetlanej mapy może się również odbywać w sposób automatyczny – w zależności od stanu poszczególnych elementów systemu (np. wyłącznie w razie alarmu w określonej lokalizacji).

System integrujący ma dostosowywalny interfejs graficzny użytkownika, oparty na standardzie HTML5, co daje możliwość m.in. umieszczenia logo użytkownika końcowego, zmiany kolorystyki, czy umieszczenia w obrębie interfejsu dowolnego elementu, zgodnego ze standardem HTML (np. formularzy).

W obrębie interfejsu, na etapie konfiguracji, możliwe jest dodanie licznych elementów, ułatwiających pracę z systemem – jak np. przyciski sterujące, liczniki, czy formularze:

- Przyciski sterujące będą mogły wykonywać jeden bądź wiele rozkazów na jednym bądź wielu urządzeniach (np. przycisk, za pomocą którego operator będzie mógł otworzyć wybraną grupę drzwi w obiekcie na stałe).
- Utworzenie liczników umożliwi wyświetlenie liczby urządzeń, będących w określonym stanie (np. wszystkie czujki pożarowe w usterce, wszystkie czujki pożarowe w stanie zabrudzenia).

W razie dowolnego alarmu system umożliwi przedstawienie operatorowi procedur postępowania. Procedury te mogą być dowolnie dostosowane, w zakresie treści, kolorystyki, czy układu, w oparciu o standard HTML. W ramach dokumentu procedury postępowania możliwe jest przygotowanie pól, dla których wymagane będzie wpisanie przez operatora komentarza na temat alarmu lub wyświetlenie przycisków sterujących, usprawniających obsługę alarmu. Wpisany przez operatora komentarz jest zachowywany w rejestrze zdarzeń, umożliwiając szczegółową analizę sytuacji nietypowej w późniejszym terminie. Procedury postępowania wspierają obsługę makr, dzięki czemu w dokumencie mogą być w sposób dynamiczny wyświetlane informacje na temat danego zdarzenia/alarmu, w tym data/czas, stan, lokalizacja.

System daje możliwość automatycznego drukowania, np. w razie alarmu, dowolnego pliku, w tym np. procedury postępowania, mapy, czy schematu.

Dziennik zdarzeń jest przechowywany w bazie danych SQL. W razie potrzeby możliwe jest wykorzystanie dowolnej, zewnętrznej instancji SQL – np. w celu znacznego zwiększenia pojemności. Dzięki wykorzystaniu otwartego standardu SQL możliwe jest tworzenie na potrzeby użytkownika dowolnych raportów systemowych, jak również połączenie z bazą danych z poziomu aplikacji zewnętrznej.

System umożliwia zastosowanie nieograniczonej liczby zintegrowanych stacji operatorskich, przy czym do 80 stacji klienckich może pracować jednocześnie dla danego serwera logowania. Interfejs klienta jest uruchamiany za pośrednictwem przeglądarki, w związku z czym nie ma konieczności instalowania dedykowanej aplikacji klienckiej. Każda aktualizacja oprogramowania serwerowego powoduje również automatyczną aktualizację interfejsu klienckiego.

Oprogramowanie ma również mieć możliwość pracy w architekturze wielu serwerów (do 10), współpracujących ze sobą. Serwer nadrzędny ma mieć możliwość odbierania informacji o stanach wszystkich elementów oraz posiadać dostęp do baz danych serwerów podrzędnych. Urządzenia,

zainstalowane w lokalizacjach rozproszonych mogą być sterowane zarówno przez operatorów lokalnych, jak i przez operatorów, zalogowanych do serwera centralnego. W razie utraty komunikacji sieciowej pomiędzy serwerami, każdy z nich musi mieć możliwość autonomicznej pracy na poziomie lokalnym.

System wspiera centralne zarządzanie alarmami lub daje możliwość dystrybucji alarmów pomiędzy stacjami operatorskimi lub operatorami. Alarmy ze wszystkich podsystemów są wyświetlane w kolejce, gdzie zawarte są przynajmniej następujące informacje:

- Data/godzina alarmu
- Stan alarmowy
- Stan bieżący elementu
- Lokalizacja alarmu
- Operator, obsługujący alarm, gdy został on potwierdzony

Wyświetlanie alarmów odbywa się w kolejności chronologicznej lub w zależności od priorytetu danego zdarzenia. System daje możliwość obsługi maksymalnie do 5000 alarmów/zdarzeń jednocześnie. System obsługuje minimum 500 zdarzeń na sekundę, również w sposób długotrwały.

Licencjonowanie oprogramowania odbywa się w oparciu o licencję elektroniczną. Dzięki temu, po przypisaniu licencji do danego komputera, istnieje możliwość łatwej jej zmiany lub rozbudowy, poprzez dokupienie i elektroniczną aktywację kolejnych pozycji. Nie jest wykorzystywany klucz sprzętowy USB, który może ulec uszkodzeniu lub zagubieniu.

INTEGRACJA SYSTEMU KONTROLI DOSTĘPU

Oprogramowanie powinno cechować się w pełni zintegrowanym modułem kontroli dostępu. Oznacza to, że powinno w swoim interfejsie użytkownika zapewniać zarówno wizualizację, konfigurację, sterowanie zdalne z map wizualizacyjnych jak i zarządzanie użytkownikami, kartami oraz uprawnieniami. Do konfiguracji i obsługi systemu kontroli dostępu nie jest zatem wymagany żaden dodatkowy serwer czy oprogramowanie.

System kontroli dostępu zapewnia wysoki stopień niezawodności, dzięki pracy w architekturze 3-warstwowej. Poza serwerem nadrzędnym systemu integrującego, istnieje możliwość wydzielenia serwera warstwy drugiej, służącego do wymiany informacji, pomiędzy kontrolerami systemu KD. W razie wyłączenia lub awarii połączenia sieciowego serwera nadrzędnego, serwer warstwy drugiej zapewnia komunikację między kontrolerami, w tym funkcji globalnych, jak np. anti-passback. Ponadto, system daje możliwość zastosowania redundantnego serwera warstwy drugiej, automatycznie przejmującego funkcje i komunikację, w przypadku awarii serwera podstawowego.

Oprogramowanie daje możliwość centralnego zarządzania kartami dla instalacji rozproszonych. Istnieje możliwość zarządzania wszystkimi kartami i uprawnieniami w systemie rozproszonym z poziomu serwera centralnego. Wszelkie zmiany, wprowadzone na poziomie globalnym, są automatycznie dystrybuowane do lokalizacji podrzędnych. Ponadto, system daje możliwość centralnego monitorowania zdarzeń i alarmów ze wszystkich serwerów podrzędnych.

System będzie umożliwiać podział całego systemu na maksymalnie 99 stref najemców. Operatorzy poszczególnych stref będą w stanie zarządzać tylko grupami użytkowników kart przynależących do danych stref. Będą mogli również przydzielać uprawnienia do przejść znajdujących się tylko we własnych strefach. W analogiczny sposób, system będzie ograniczał dostęp do przeglądania logów zdarzeń tylko ze stref, do których operatorzy mają uprawnienia. Ponadto, każdy operator może przydzielić uprawnienia do przejść, znajdujących się w strefie wspólnej, jak np. wejście do budynku czy lobby.

System daje możliwość dodawania nowych kart użytkowników, przy pomocy dowolnego czytnika kontroli dostępu. Ponadto, możliwe jest dostosowanie pól i elementów okna dialogowego, służącego

do wprowadzania nowych użytkowników do systemu. System umożliwia też projektowanie układu graficznego kart, w tym dodawanie kodów kreskowych oraz kodów QR.

Skalowalność systemu kontroli dostępu powinna umożliwiać dowolną rozbudowę do przynajmniej:

- 400 000 kart,
- 10 000 przejść kontrolowanych,
- 1000 grup uprawnień,
- 1200 kontrolerów.

System daje możliwość automatycznego generowania logów na potrzeby zewnętrznego systemu RCP, z dowolnych czytników w systemie (nie są wymagane do tego dodatkowe, dedykowane czytniki). Logi są zapisywane w łatwej do importowania formie pliku tekstowego.

System posiada ogólnodostępny interfejs SDK/API, umożliwiający zarządzanie personelem systemu kontroli dostępu (użytkownikami, kartami, uprawnieniami) poprzez zewnętrzną aplikację – np. na potrzeby systemów RCP, kadrowych, zarządzania parkingiem czy gośćmi.

INTEGRACJA SYSTEMU CCTV

Oprogramowanie integrujące posiada zaimplementowaną integrację systemu CCTV. Integracja ta umożliwia skorelowanie obrazów na żywo dla wybranych kamer, z alarmami z innych zintegrowanych systemów (np. wyświetlenie operatorowi obrazów na żywo, w momencie wystąpienia alarmu pożarowego, włamania lub sforsowania drzwi itp.).

System umożliwia bezpośredni dostęp z poziomu przeglądarki zdarzeń do zarchiwizowanego materiału wideo z kamer, enkoderów, rejestratorów czy macierzy dyskowych, dotyczących danego zdarzenia. W przypadku kamer PTZ możliwe jest sterowanie kamery bezpośrednio z poziomu systemu integrującego.

INTEGRACJA SYSTEMU POŻAROWEGO

System zapewnia integrację systemu sygnalizacji pożarowej i wizualizację na mapach stanu wszystkich jego elementów. Umożliwia to przykładowo, w przypadku alarmu pożarowego, automatyczne wysterowanie elementów systemu alarmowego, kontroli dostępu i wyświetlenie obrazu z kamery.

System daje możliwość rozróżnienia alarmu pożarowego 1-go i 2-go stopnia i różnego rodzaju reakcje automatyczne, w zależności o rodzaju alarmu, czy też jego źródła.

System może informować o stanie zabrudzenia czujek pożarowych. Umożliwia to automatyczne informowanie operatora o ilości elementów, wymagających konserwacji.

INTEGRACJA SYSTEMY SYGNALIZACJA WŁAMANIA I NAPADU

Oprogramowanie powinno umożliwiać wizualizowanie stanów urządzeń w systemie SSWiN takich jak: strefa gotowa do zazbrojenia, strefa niegotowa do zazbrojenia, strefa zazbrojona, strefa niezazbrojona, czujka w alarmie, usterka.

Oprogramowanie powinno umożliwiać również sterowanie urządzeniami w systemie SSWiN jak np.: zazbrojenie/rozbrojenie strefy, aktywacja/dezaktywacja przekaźnika, aktywacja/ dezaktywacja wyjścia typu OC.

Bilans mocy kontrolerów

n_i	spodziewana liczba uruchomień zamka na godzinę
t_{acti}	czas pobudzenia dla zamków typu fail-secure
I_{equip}	Pobór prądu przez urządzenia (bez zamków)
$I_{fail-safe}$	Pobór prądu przez zamki typu fail-secure
$I_{fail-secure}$	Pobór prądu przez zamki typu fail-safe

D_i Cykl pracy (procent uruchomień na godzinę)
 I_{avg} średnie obciążenie dla przewidywanych warunków obciążenia
 C Minimalna pojemność akumulatora

$$D_i = t_{acti} \times n_i / 3600$$

$$I_{fail-safe} = \text{suma}(I_{fail-safe})$$

$$I_{fail-secure} = \text{suma}(D_i \times I_{fail-securei})$$

$$I_{avg} = I_{equip} + I_{fail-secure} + I_{fail-safe}$$

$$C = 1,2 \times t \times I_{avg}$$

KD01

	Ilość	I _{fail-secure_i}	I _{fail-safe_i}	t _{acti}	n	D _i	I _{fail-secure}	I _{fail-safe}
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep rewersyjny	4	0	0,17	2	100	5,56%	0,000	0,680
Suma:							0,000	0,680

	Ilość	I _{equip_i}	Suma I _{equip_i}
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	7	0,065	0,455
		I _{equip} =	0,955

$$I_{avg} = 1,635 \text{ A}$$

GRADE 3		
t =	2	h
C =	3,9	Ah

GRADE 4		
t =	4	h
C =	7,8	Ah

KD02

	Ilość	I _{fail-secure_i}	I _{fail-safe_i}	t _{acti}	n	D _i	I _{fail-secure}	I _{fail-safe}
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep rewersyjny	4	0	0,17	2	100	5,56%	0,000	0,680
Suma:							0,000	0,680

	Ilość	I _{equip_i}	Suma I _{equip_i}
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	8	0,065	0,52
		I _{equip} =	1,02

$$I_{avg} = 1,700 \text{ A}$$

GRADE 3		
t =	2	h
C =	4,1	Ah

GRADE 4		
t =	4	h
C =	8,2	Ah

KD03

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep rewersyjny	4	0	0,17	2	100	5,56%	0,000	0,680
Suma:							0,000	0,680

	Ilość	Iequip_i	Suma Iequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	7	0,065	0,455
		Iequip =	0,955

Iavg= 1,635 A

GRADE 3		
t =	2	h
C=	3,9	Ah

GRADE 4		
t =	4	h
C=	7,8	Ah

KD04

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep rewersyjny	5	0	0,17	2	100	5,56%	0,000	0,850
Suma:							0,000	0,850

	Ilość	Iequip_i	Suma Iequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	6	0,065	0,39
		Iequip =	0,89

Iavg= 1,740 A

GRADE 3		
t =	2	h
C=	4,2	Ah

GRADE 4		
t =	4	h
C=	8,4	Ah

KD05

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep rewersyjny	4	0	0,17	2	100	5,56%	0,000	0,680
Suma:							0,000	0,680

	Ilość	Iequip_i	Suma Iequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	7	0,065	0,455
		Iequip =	0,955

lavg= 1,635 A

GRADE 3		
t =	2	h
C=	3,9	Ah

GRADE 4		
t =	4	h
C=	7,8	Ah

KD06

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep reweryjny	7	0	0,17	2	100	5,56%	0,000	1,190
						Suma:	0,000	1,190

	Ilość	Iequip_i	Suma Iequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	8	0,065	0,52
		Iequip =	1,02

lavg= 2,210 A

GRADE 3		
t =	2	h
C=	5,3	Ah

GRADE 4		
t =	4	h
C=	10,6	Ah

KD07

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep reweryjny	6	0	0,17	2	100	5,56%	0,000	1,020
						Suma:	0,000	1,020

	Ilość	Iequip_i	Suma Iequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	7	0,065	0,455
		Iequip =	0,955

lavg= 1,975 A

GRADE 3		
t =	2	h
C=	4,7	Ah

GRADE 4		
t =	4	h
C=	9,5	Ah

KD08

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep reweryjny	3	0	0,17	2	100	5,56%	0,000	0,510
						Suma:	0,000	0,510

	licz	lequip_i	Suma lequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	6	0,065	0,39
		lequip =	0,89

lavg= 1,400 A

GRADE 3		
t =	2	h
C =	3,4	Ah

GRADE 4		
t =	4	h
C =	6,7	Ah

KD09

	licz	lfail- secure_i	lfail-safe_i	tacti	n	Di	lfail- secure	lfail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep reweryjny	6	0	0,17	2	100	5,56%	0,000	1,020
						Suma:	0,000	1,020

	licz	lequip_i	Suma lequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	6	0,065	0,39
		lequip =	0,89

lavg= 1,910 A

GRADE 3		
t =	2	h
C =	4,6	Ah

GRADE 4		
t =	4	h
C =	9,2	Ah

KD10

	licz	lfail- secure_i	lfail-safe_i	tacti	n	Di	lfail- secure	lfail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep reweryjny	6	0	0,17	2	100	5,56%	0,000	1,020
						Suma:	0,000	1,020

	licz	lequip_i	Suma lequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	7	0,065	0,455
		lequip =	0,955

lavg= 1,975 A

GRADE 3		
t =	2	h
C=	4,7	Ah

GRADE 4		
t =	4	h
C=	9,5	Ah

KD11

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep reweryjny	5	0	0,17	2	100	5,56%	0,000	0,850
Suma:							0,000	0,850

	Ilość	Iequip_i	Suma Iequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	8	0,065	0,52
		Iequip =	1,02

Iavg= 1,870 A

GRADE 3		
t =	2	h
C=	4,5	Ah

GRADE 4		
t =	4	h
C=	9,0	Ah

KD12

	Ilość	Ifail-secure_i	Ifail-safe_i	tacti	n	Di	Ifail-secure	Ifail-safe
		[A]	[A]	[s]		[%]	[A]	[A]
Elektrozaczep reweryjny	4	0	0,17	2	100	5,56%	0,000	0,680
Suma:							0,000	0,680

	Ilość	Iequip_i	Suma Iequip_i
AMC2 Kontroler RS485 z Kartą CF	1	0,25	0,25
AMC2 rozszerzenie 8we/8wy	1	0,25	0,25
Czytnik LECTUS duo 3000, MiFare DesFire	5	0,065	0,325
		Iequip =	0,825

Iavg= 1,505 A

GRADE 3		
t =	2	h
C=	3,6	Ah

GRADE 4		
t =	4	h
C=	7,2	Ah

6 Instalacja SSWiN

W budynku zastosowano całkowity system ochrony SSWiN1 i SSWiN2 (kancelaria tajna) które spełniają wymagania drugiego (pomieszczenia biurowe, techniczne) i trzeciego poziomu (kancelaria tajna).

Podział na poziomy dostęp:

Wejścia do budynku, pomieszczenia biurowe, pomieszczenia techniczne: Stopień zabezpieczenia 2. Kontrola dostępu dwustronna lub jednostronna, czujniki alarmowe, zabezpieczenie otwarcia okien i drzwi

Wejścia do pomieszczeń wspólnych (łazienki, pokój gościnny, pokój matki z dzieckiem, sala konf, pok. Socjalny) poziom 1, brak kontroli dostępu, pomieszczenia z oknami zabezpieczone przed otwarciem, czujniki ruchu.

Wejścia do kancelarii tajnej i serwerowni: Stopień zabezpieczenia 3. Dwustronna kontrola dostępu, zabezpieczenie okien i drzwi przed otwarciem i penetracją (czujniki zbitcia szyby, czujniki ruchu z antymaskingiem, kamera przed wejściem z funkcjami biometrycznymi, dodatkowy wideodomofon)

Nowa centrala zlokalizowana będzie przy wejściu głównym do budynku w pomieszczeniu 0.04.

W pomieszczeniach zespołu pomieszczeń KT (kancelarii tajnej) zgodnie z wytycznymi inwestora będzie wydzielony odrębny system alarmowy z centralką i urządzeniami alarmowymi. Uzbrojenie i rozbrojenie alarmu każdorazowo przez kierownika KT i pracownika KT. Manipulator systemowy zostanie zainstalowany w korytarzu, przed wejściem do KT.

Na parterze przy wejściach 0.01 i 0.20 zlokalizowane zostaną główne manipulatory systemowe z wyświetlaczem. Instalację należy prowadzić w korytkach teletechnicznych oraz rurkach instalacyjnych pod tynkiem. Rzut instalacji i schemat połączeniowy został zamieszczony na rysunkach.

Należy przewidzieć możliwość zastosowania różnych systemów

Wszystkie okna należy wyposażyć w kontaktrony (sterowanie klimatyzacją oraz sygnalizujące otwarcie okna do centrali alarmowej. Urządzenia zostaną podłączone do centrerek alarmowych poprzez moduły rozszerzające. Dodatkowo zostały zastosowane 2 piloty/przyciski antynapadowe zlokalizowane w pomieszczeniach kancelarii tajnej.



Stosowane są moduły rozszerzające LSN

- do podłączania 6 stref czujek (czujki konwencjonalne lub wejścia czujek monitorujących)
- stosowanych do celów kontrolnych (4 wyjścia sterowania)
- do podłączania urządzeń uzbrajających (np. NBS 10) i powiązanych podzespołów systemowych

do lokalnej sieci bezpieczeństwa (LSN).

- ▶ Podłączanie 6 stref czujek (czujki konwencjonalne lub wejścia czujek monitorujących)
- ▶ Podłączanie 4 wolnych wyjść sterowania
- ▶ Podłączanie urządzeń uzbrajających (np. NBS 10) i powiązanych podzespołów systemowych
- ▶ Monitorowanie podstawowych linii alarmowych, zwarc lub przerwania przewodów.
- ▶ Rozbudowany system ograniczania wartości w „wersji udoskonalonej” w trybie LSNI.

Informacja z otwarcia okna zostanie przesłana do serwera BMS który umożliwi sterowanie załączaniem/wyłączaniem grzejników poprzez zawory i regulatory temperatury jak również wyłączanie klimatyzatorów w pomieszczeniu.

Centrala alarmowa SSWiN1 i SSWiN2

System sygnalizacji włamania i napadu SSWiN1 wyposażony będzie w centralę, zgodną z normami serii PN-EN50131 dla urządzeń poziomu 2 i 3, adresowalną, wyposażoną w odpowiedni zasilacz, niezbędne do pracy karty funkcyjne, interfejsy sterujące i transmisyjne, panel wyświetlacza w języku polskim. Centrala CCWiN2 wyposażona będzie dla urządzeń poziomu 3.

Zastosowane rozwiązanie musi być w pełni adresowalne tzn. można łatwo zidentyfikować każdy element systemu alarmowego oraz określić jego stan bez potrzeby stosowania dodatkowych elementów adresowalnych.

Obsługa poszczególnych stref systemu, powinna odbywać się lokalnie z manipulatorów, pozwalających na uzbrajanie/rozbrajanie danej strefy, przez osobę do tego upoważnioną. Jednocześnie system wyposażony będzie w komunikację TCP/IP oraz posiadać będzie zintegrowany serwer OPC gwarantujący pełną integrację w oprogramowaniu BMS.

W pomieszczeniach budynku będą zainstalowane urządzenia detekcyjne m.in. takie jak:

- czujki dualne: pasywne podczerwieni + mikrofalowe z antymaskingiem (poziom 3)
- czujki pasywne podczerwieni (poziom 2)
- kontaktrony (magnetyczne) na wszystkich drzwiach prowadzących do wydzielonych obszarów alarmowania i otwieranych skrzydłach okiennych
- przyciski - ostrzegacze napadowe w wydzielonych strefach.

Do rozgłaszania sygnałów alarmowych projektuje się zainstalować sygnalizatory optyczno – akustyczne z opcją tylko optyczną wewnętrzną i optyczno – akustyczne zewnętrzne.

Wymagania w zakresie funkcjonalności systemu SSWiN:

- narzędzia do importu/exportu bazy danych oraz importu/exportu pełnej konfiguracji systemu
- możliwość importu/exportu wybranych danych z systemu (możliwość definiowania wybranych danych)
- możliwość integracji z nadrzędnym systemem BMS poprzez
- możliwość tworzenia obszarów logicznych / stref (np. pojedynczych pomieszczeń, grup pomieszczeń, całych pięter)
- możliwość nadawania uprawnień operatorom do określenia elementów systemu
- narzędzie do wyszukiwania pozwalające uprawnionym użytkownikom systemu sprawdzić wszystkie zdarzenia
- raporty/wydruki zgodnie z podanymi parametrami wyszukiwania w odniesieniu do osób, miejsca i czasu

- powiadamianie, możliwość przekazywania wygenerowanych alarmów za pośrednictwem poczty elektronicznej oraz SMS (forma tekstowa o wystąpieniu zdarzenia wraz z treścią alarmu).

Zaprojektowany system opiera swoje działanie o technologię LSN. Technologia Local Security Network (LSN) umożliwia bezprzerwową pracę nawet w przypadku usterki. Elementy detekcyjne są łączone pętlowo. System wykrywa automatycznie każde urządzenie i przypisuje mu miejsce (adres) na pętli. W przypadku uszkodzenia jednego z urządzeń lub przerwania pętli system pracuje dalej. System może być w pełni zintegrowany przez sieć IP z systemem zarządzania w rodzaju zintegrowanego systemu zarządzania budynkiem.

Pojedynczy system obsługuje maksymalnie 8 modułów pętlowych. Do każdego z nich można dołączyć do 127 elementów wykonanych w technologii LSN. Długość jednej pętli LSN wynosi maksymalnie 1000 m, a jej maksymalna obciążalność wynosi 300 mA. Okablowanie pętli musi być wykonane z przewodu ekranowanego o przekroju 0,6-1,0 mm. Istnieje możliwość prowadzenia dodatkowego zasilania do dołączanych do pętli elementów z dwóch niezależnych źródeł AUX, w które wyposażony jest każdy moduł LSN. Obciążalność każdego ze źródeł wynosi 500 mA.

Kolejne moduły LSN można wykorzystywać poza magistralą wewnętrzną, którą prowadzi się w obudowie głównej. Magistrala zewnętrzna ma maksymalną długość wynoszącą 1000 m. Wykonuje się ją z przewodu ekranowego lub nieekranowanego o średnicy 0,6-1,0 mm. Do każdej wyniesionej lokalizacji, w której ma znajdować się wyniesiony moduł LSN należy doliczyć wyniesioną obudowę rozszerzeń, zasilacz, a także dwa akumulatory 12 V o pojemności 17 Ah każdy. W jednej wyniesionej obudowie rozszerzeń można umieścić maksymalnie dwa moduły LSN.

Manipulatory systemu można podłączać do magistrali wewnętrznej (znajdującej się wewnątrz obudowy) lub też do magistrali zewnętrznej.

Poniżej znajdują się informacje na temat elementów składowych systemu.

Czujka dualna PIR/MW z antymaskingiem

- Standardowy zasięg 12 x 12 m, możliwość wyboru krótkiego zasięgu 8 x 10 m
- TriTech. Technologia pasywnej podczerwieni oraz mikrofalowy radar Dopplerowski z technologią FSP (First Step Processing)
- Adaptacyjne przetwarzanie mikrofalowe zakłóceń – zmniejszona liczba alarmów wywoływanych powtarzającymi się sygnałami
- Technologia wielopunktowego antymaskingu ze zintegrowanym wykrywaniem zablokowania soczewki sprayem — wykrywa próby ograniczenia pola widzenia czujki
- Technologia wykrywania maskowania i kamuflażu (C2DT)
- Praca w sieci LSN – dwustronna komunikacja z centralą alarmową topologia pętli
- Zakres napięć zasilania: od 9 do 29VDC
- Zdalny autotest
- Technologia przetwarzania sygnałów z kilku detektorów
- Trójogniskowy układ optyczny zapewniający trzy długości ogniskowania: soczewka dalekiego, średniego i krótkiego zasięgu
- Aktywna redukcja białego światła
- Dynamiczna kompensacja temperaturowa
- Stopień zabezpieczenia Grade 3

Czujka kontaktronowa

- Styk magnetyczny do montażu powierzchniowego do monitorowania otwarcia drzwi i okien
- Nadzór antysabotażowy
- Klasa środowiskowa (EN 50130-5) III
- Stopień zabezpieczenia Grade 3

Panel główny (wyłącznie do montażu na magistrali wewnętrznej):

Jako część modułowej centrali alarmowej panel główny obsługuje szereg zastosowań przy użyciu magistrali) opartej na technologii CAN (Controller Area Network) pracującej jako szyna wewnętrzna lub zewnętrzna. Panel główny instalowany jest na odchylanej szynie montażowej w zestawie obudowy centrali.

Panel główny obsługuje maks 1500 adresów, 500 obszarów i 1000 użytkowników. Jako część modułowej centrali alarmowej panel główny komunikuje się z systemami zarządzania budynkiem. Centrala zapewnia dwie magistrale danych:

- Wewnętrzna BDB – o całkowitej długości ograniczonej do 6m, łączy panel główny z innymi urządzeniami.
- Zewnętrzna BDB – o całkowitej długości ograniczonej do 1000 m, umożliwia umieszczenie paneli sterowania i zasilaczy w wymaganych punktach użytkowania, zapewniając większą skuteczność.

Wejścia i wyjścia

Panel główny obsługuje jedno nienadzorowane wejście tampera i osiem wejść nadzorowanych. Obsługuje również jedno wyjście funkcji dodatkowej, dwa wyjścia przekaźnikowe ze stykami beznapięciowymi typu C oraz dwa programowalne wyjścia do lokalnych urządzeń powiadamiających.

Wyjście funkcji dodatkowej oraz oba wyjścia zasilania posiadają zabezpieczenie nadprądowe. Wyjścia zapewniają indywidualne zabezpieczenie, co oznacza, że w przypadku zwarcia obwodu na jednym wyjściu awaria nie wpływa na działanie drugiego wyjścia.

Manipulator (do montażu na magistrali wewnętrznej i zewnętrznej)

Ekran dotykowy - 14 cm (5,7") LCD z regulowanym podświetleniem LED

Interfejs graficzny (16-bitowa paleta barw przy rozdzielczości (320 x 240 pikseli) składający się z intuicyjnych ikon i menu

Wersje językowe do wyboru przez użytkownika

Wbudowany głośnik z regulowaną głośnością

Brak odsłoniętych części przy dostępie do zacisków; okablowanie w podstawie dołączane do zacisków wciskanych

Ekran dotykowy

Centrum sterowania posiada rezystancyjny ekran dotykowy, który służy do wprowadzania danych do systemu bez konieczności używania tradycyjnych przycisków. Zapewnia to elastyczną prezentację dostępnych funkcji i intuicyjną interakcję z grafikami i ikonami ekranowymi. Technologia wyświetlacza ciekłokrystalicznego z tranzystorami cienkowarstwowymi (TFT-LCD) zapewnia znakomitą jakość obrazu. Hermetycznie obudowany układ elektroniczny zabezpiecza przed fizycznym uszkodzeniem w czasie obsługi i instalacji.

Sygnały dźwiękowe

Panel sterowania posiada głośnik generujący następujące sygnały:

- Sygnał naciśnięcia właściwego przycisku: potwierdzenie dokonania wyboru poprzez naciśnięcie obrazu na ekranie dotykowym.
- Sygnał niewłaściwego wyboru: wskazanie naciśnięcia nieaktywnego przycisku lub pola bez obrazu przycisku.
- Sygnał opóźnienia wejścia: powiadomienie o rozbrojeniu systemu w zaprogramowanym czasie
sygnał opóźnienia wyjścia: powiadomienie o przygotowaniu do uzbrojenia systemu w zaprogramowanym czasie.
- Sygnał alarmu włamaniowego: wskazanie warunku alarmowego.
- Sygnał nadzoru włamaniowego: wskazanie warunku nieprawidłowości (problemu) nadzorowanego punktu.
- Sygnał problemu włamaniowego: wskazanie warunku nieprawidłowości (problemu) punktu.
- Gong: wskazanie uaktywnienia punktu.
- Sygnał problemu systemowego: wskazanie warunku problemu systemowego w rodzaju awarii sieci energetycznej.

Moduł LSN (do montażu na magistrali wewnętrznej i zewnętrznej):

Cechy użytkowe

- Obsługa maks. 127 urządzeń LSN przy maksymalnym obciążeniu pętli prądowej LSN wynoszącym 300 mA
- Możliwość stosowania elastycznych struktur sieciowych (jedna pętla lub dwa odgałęzienia)
- Pojedyncza nadmiarowość na wypadek awarii w konfiguracjach pętli (nie ma zastosowania w konfiguracji odgałęzień)
- Dwa wyjścia zasilania zewnętrznego (500 mA każde)

Każdy moduł łączy jedną pętlę lokalnej sieci bezpieczeństwa (Local SecurityNetwork - LSN) lub dwa odgałęzienia przy maks. prądzie wyjściowym 300 mA i obsługuje maks. 127 urządzeń LSN. Modułowa centrala alarmowa obsługuje maks. osiem modułów na zewnętrznej magistrali oraz maks. 1500 adresów.

Do ochrony wnętrza pomieszczeń należy zastosować pasywne czujki podczerwieni oraz czujki dualne. Zaleca się zastosowanie czujek wyposażonych w funkcję antymaskingu dla zapewnienia wyższego poziomu ochrony.

Moduł rozszerzeń centrali

- Podłącza się do 6 obszarów wykrywania (czujki konwencjonalne lub monitorujące wejścia alarmowe), 4 beznapięciowych wyjść sterujących
- Monitoruje linię główną pod kątem występowania alarmu, zwarcia i przerwy
- Rozbudowane systemowe wartości graniczne w LSNi
- Styk antysabotażowy (alarm antysabotażowy) i zintegrowany sygnalizator dźwiękowy
- Można zainstalować maks. 2 moduły przekaźnika IMS-RM i ścienny styk antysabotażowy
- Minimalne napięcie robocze (V DC) 15
- Maksymalne napięcie robocze (V DC) 33
- Maksymalny pobór prądu (mA) 4.95

Zewnętrzny sygnalizator akustyczno – optyczny

Cechy szczególne:

- Typ produktu Sygnalizator optyczno-akustyczny
- Stopień zabezpieczenia Grade 3
- Zabezpieczenie oderwania od podłoża

- Zabezpieczenie przed ingerencją w produkt
- Kolor klosza Biały, Czerwony, Niebieski, Zielony
- Kolor obudowy Biały Czarny
- Natężenie dźwięku (dB) <120
- Rezerwowe źródło zasilania
- Zasilanie 12VDC
- Temperatura pracy (°C) -25...+55
- Wymiar wysokość (mm) 290
- Wymiar szerokość (mm) 186
- Wymiar głębokość (mm) 58
- Rodzaj sygnalizacji Akustyczno-optyczna

Czujnik zbitcia szyby

W każdym oknie w obszarze zespołu pomieszczeń KT zostaną zastosowane czujniki zbitcia szyby wg rysunków. Dzięki zastosowaniu mikroprocesorowej technologii analizy dźwięku (SAT) do rozpoznawania określonych częstotliwości towarzyszących stłuczeniu szkła, czujka potrafi precyzyjnie wykrywać stłuczenie szyb wykonanych ze szkła zwykłego, hartowanego, laminowanego lub zbrojonego siatką drucianą.

Mikroprocesor analizuje sygnały dźwiękowe bazując na technologii analizy dźwięku SAT, która analizuje określone częstotliwości, taktowania i charakterystyki. Ta zaawansowana technologia przetwarzania gwarantuje skuteczność wykrywania, eliminując jednocześnie fałszywe alarmy.

Standardowy obszar pokrycia to 7,6 m w przypadku powierzchni szklanych o rozmiarze 30,5 x 30,5 cm.



SPECYFIKACJA TECHNICZNA

PARAMETRY ELEKTRYCZNE	
Pobór prądu	23 mA przy napięciu 12 VDC
Napięcie	6 – 15 VDC
PARAMETRY ŚRODOWISKOWE	
Temperatura pracy	od -29°C do +49°C W instalacjach z certyfikatem UL: od 0°C do +49°C
Odporność na zakłócenia radiowe (RFI)	Brak alarmu lub uzbrojenia na częstotliwościach krytycznych w przedziale od 26 do 950 MHz przy natężeniu pola 50 V/m.
PARAMETRY MECHANICZNE	
Wymiary (wys. x śr.)	8,6 x 8,6 x 2,1 cm
Materiał	Udaroodporny plastik ABS
WYJŚCIA	
Alarmowe	Przełącznik kontaktronowy C o obciążalności 3,5 W, obciążenie rezystancyjne 125 mA przy napięciu 28 VDC
Przełącznik antysabotażowy	Normalnie zwarty (NC) włącznik zabezpieczający z oddzielnymi zaciskami reagujący na otwarcie pokrywy. Obciążalność maksymalna 125 mA przy napięciu 28 VDC

Bilans mocy

Tablica 23 – Minimalne okresy gotowości zasilacza rezerwowego

Typy zasilaczy	Stopień 1 h	Stopień 2 h	Stopień 3 h	Stopień 4 h
Typ A	12	12	60	60
Typ B	24	24	120	120

W I&HAS 3 i 4 stopnia, gdy uszkodzenia podstawowego źródła zasilania są zgłaszane w alarmowym centrum odbiorczym lub w innym centrum oddalonym, czas gotowości zasilacza rezerwowego może być dwukrotnie skrócony.

SSWiN1

Zakładane parametry pracy systemu (definiowane przez użytkownika)		
Czas czuwania systemu na zasilaniu rezerwowym (godziny)	30	
Czas trwania alarmu na zasilaniu rezerwowym (minuty)	30	
Zakładane obniżenie wartości znamionowych (derating)	25%	
Kalkulowane wartości	Moc w stanie czuwania (Wat)	Moc w stanie alarmu (Wat)
Elementy panelu głównego	2,69	2,24
Elementy modułu komunikacyjnego DE	0,88	1,82
Elementy zasilacza	3,36	3,36
Elementy panelu sterowania	6,40	9,92
Elementy modułów pętlowych LSN	15,09	15,65
Elementy pomocnicze GLT(Aux)	0,00	0,00
Subtotal	28,42	32,99
Zapotrzebowanie mocy	Moc (Wat - Godziny)	
Moc wymagana w czasie czuwania	838,3	
Moc wymagana w czasie alarmu	16,5	
Zapotrzebowanie mocy subtotal = czuwanie + alarm	854,8	
Zapotrzebowanie mocy - obniżenie wartości (derating)	213,7	
Łączne zapotrzebowanie mocy = Subtotal + Derating	1068,5	
ŁĄCZNE ZAPOTRZEBOWANIE AKUMULATORÓW (AMPEROGODZINY)	45	

Zasilanie 12VDC sygnalizatorów

Sygnalizator zewnętrzny opt-akust ODYSSEY X-B	6	szt.
Pobór prądu w stanie spoczynku	18	mA
Suma prądu w stanie spoczynku	108	mA
Pobór prądu w alarmie	445	mA
Suma prądu w alarmie	2670	mA
Czas podtrzymania w stanie spoczynku [h]	30	h
Czas podtrzymania w alarmie [h]	0,5	h
Obliczona pojemność akumulatorów	5,72	Ah

Dobrano zasilacz 12Vdc/5A + akumulator 12V/17Ah

HPSG3-12V5A-C

REZULTAT OCENY POPRAWNOŚCI (Pozytywny/Negatywny)					
Testy pętli LSN (Prąd 300mA max; Max. ilość urządzeń 127)					
		Obciążalność prądowa pętli (mA)	Rezultat	Ilość urządzeń	Rezultat
Pętla LSN 1		259,20	POZYTYWNY	52	POZYTYWNY
Pętla LSN 2		139,60	POZYTYWNY	28	POZYTYWNY
Pętla LSN 3		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 4		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 5		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 6		0,00	POZYTYWNY	0	POZYTYWNY

Pętla LSN 7	0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 8	0,00	POZYTYWNY	0	POZYTYWNY
Limit prądowy modułu komunikacyjnego DE (500mA)				
Drukarka + Out1 + Out2	0,00	POZYTYWNY		

UWAGA: Należy zastosować dodatkową obudowę na 4 szt. akumulatorów 40Ah i zasilacz.



Odpowiednia do zasilacza i dwóch zestawów akumulatorów 2x 12 V / 38–45 Ah

SSWiN2

Zakładane parametry pracy systemu (definiowane przez użytkownika)		
Czas czuwania systemu na zasilaniu rezerwowym (godziny)	30	
Czas trwania alarmu na zasilaniu rezerwowym (minuty)	30	
Zakładane obniżenie wartości znamionowych (derating)	25%	
Kalkulowane wartości	Moc w stanie czuwania (Wat)	Moc w stanie alarmu (Wat)
Elementy panelu głównego	3,19	2,74
Elementy modułu komunikacyjnego DE	0,88	1,82
Elementy zasilacza	5,16	3,36
Elementy panelu sterowania	3,20	4,96
Elementy modułów pętlowych LSN	2,66	2,94
Elementy pomocnicze GLT(Aux)	0,00	0,00
Subtotal	15,09	15,82
Zapotrzebowanie mocy	Moc (Wat - Godziny)	
Moc wymagana w czasie czuwania	445,2	
Moc wymagana w czasie alarmu	7,9	
Zapotrzebowanie mocy subtotal = czuwanie + alarm	453,1	
Zapotrzebowanie mocy - obniżenie wartości (derating)	113,3	
Łączne zapotrzebowanie mocy = Subtotal + Derating	566,4	
ŁĄCZNE ZAPOTRZEBOWANIE AKUMULATORÓW (AMPEROGODZINY)	24	

REZULTAT OCENY POPRAWNOŚCI (Pozytywny/Negatywny)					
Testy pętli LSN (Prąd 300mA max; Max. ilość urządzeń 127)					
		Obciążalność prądowa pętli (mA)	Rezultat	Ilość urządzeń	Rezultat
Pętla LSN 1		24,90	POZYTYWNY	5	POZYTYWNY
Pętla LSN 2		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 3		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 4		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 5		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 6		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 7		0,00	POZYTYWNY	0	POZYTYWNY
Pętla LSN 8		0,00	POZYTYWNY	0	POZYTYWNY
Limit prądowy modułu komunikacyjnego DE (500mA)					
Drukarka + Out1 + Out2		0,00	POZYTYWNY		

7 Rozłączanie klimatyzacji po otwarciu okna

Automatyczne wyłączanie klimatyzatorów przy otwarciu okna w poszczególnych pomieszczeniach będzie realizowane poprzez system BMS. Kontraktony okienne połączone z interfejsami komunikacyjnymi systemu SSWiN będą posiadały adres. BMS po otrzymaniu sygnału o otwarciu okna przekaże informacje do klimatyzatorów w celu ich wyłączenia.

Tabela adresowania kontraktonów przyporządkowanych poszczególnym pomieszczeniom:

Interfejs komunikacyjny	Kontrakton	Pomieszczenie
LS1.4	1.4.1	0,04
	1.4.2	
LS1.6	1.6.2	0,06
	1.6.3	
	1.6.4	
	1.6.5	
	1.6.1	0,11
LS1.15	1.15.1	0,15
	1.15.2	
	1.15.3	0,21
	1.15.4	
LS1.21	1.21.3	0,26
	1.21.4	
	1.21.5	0,27
	1.21.6	
LS1.16	1.16.1	0,28
	1.16.2	0,28
LS1.10	1.10.1	0,30
	1.10.2	
LS1.24	1.24.1	1,20
	1.24.2	
	1.24.5	1,21
	1.24.6	
LS1.27	1.27.1	1,19
	1.27.2	

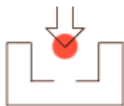
	1.27.3	1,18
	1.27.4	
	1.27.5	1,17
	1.27.6	
	1.27.7	
	1.27.8	
LS1.30	1.30.1	1,13
	1.30.2	
	1.30.3	1,12
	1.30.4	
	1.30.5	
LS1.36	1.36.1	1,10
	1.36.2	
	1.36.3	
	1.36.4	
LS1.37	1.37.1	1,11
	1.37.2	
	1.37.3	1,08
	1.37.4	
	1.37.5	
	1.37.6	
LS1.39	1.39.1	1,04
	1.39.2	
	1.39.3	
	1.39.4	
	1.39.5	
	1.39.6	
LS2.5	2.5.1	KT
	2.5.2	
	2.5.3	Czytelnia KT
	2.5.4	
LS1.44	1.44.3	1,26
	1.44.4	
LS1.47	1.47.1	1,22
	1.47.2	
	1.47.3	1,23
	1.47.4	
	1.47.5	1,24
	1.47.6	
LS1.79	1.79.1	2,24
	1.79.2	
	1.79.5	2,25
	1.79.6	
LS1.54	1.54.1	2,23
	1.54.2	
	1.54.5	2,21
	1.54.6	
LS1.57	1.57.1	2,20

	1.57.2	2,19
	1.57.3	
	1.57.4	
	1.57.5	2,15
	1.57.6	
	1.57.7	
LS1.65	1.65.1	2,10
	1.65.2	
	1.65.3	
	1.65.4	
LS1.66	1.66.1	2,07
	1.66.2	
	1.66.3	
	1.66.4	
LS1.70	1.70.3	2,30
	1.70.4	
LS1.74	1.74.1	2,26
	1.74.2	2,27
	1.74.3	
	1.74.4	2,28
	1.74.5	
	1.74.6	

8 Access Point Wi-Fi

W obiekcie należy zainstalować punkty dostępowe Wi-Fi.
Parametry techniczne zamieszczono poniżej:





Urządzenie do zastosowań wewnętrznych

Wewnętrzne urządzenia sieciowe zostały zaprojektowane z myślą o infrastrukturach bezprzewodowych działających w zadanych pomieszczeniach. Takie urządzenia idealnie nadają się do rozbudowy prywatnych sieci domowych oraz biurowych. Materiały oraz komponenty zastosowane w punkcie dostępowym nie pozwalają na pracę w miejscach, gdzie panują trudne warunki pogodowe.

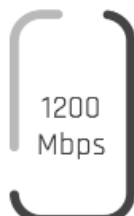


Wysoka przepustowość i najlepsza jakość sieci dzięki WiFi szóstej generacji

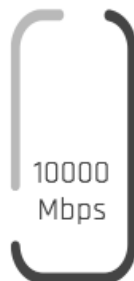
Standard ten reprezentuje szóstą generację sieci bezprzewodowych. Technologia wykorzystuje częstotliwości 2,4 GHz oraz 5 GHz. Niekwestionowanym atutem takiego rozwiązania jest kapitalna szybkość połączenia nawet przy dużej liczbie urządzeń. Access point, który pracuje w standardzie 802.11ax znajduje szerokie zastosowanie zarówno w domu, jak i w biurze, zapewniając wygodę użytkownika na najwyższym poziomie.



802.11ax



WiFi AC



WiFi AX



Najwyższy poziom ochrony dzięki nowej technologii WPA3

WPA3 To nowoczesny standard szyfrowania stosowany w infrastrukturach bezprzewodowych, który zastąpił popularną dotąd technologię WPA2. Dzięki zastosowaniu 192-bitowego kodu szyfrującego, użytkownicy mogą liczyć na najwyższy poziom bezpieczeństwa w sieci, co dziś stanowi niezwykle ważny aspekt. Takie rozwiązanie sprawdzi się znakomicie zarówno w biurze, jak i w domu. Wybierz zaawansowany model i ciesz się komfortem korzystania z internetu każdego dnia.



Koniec ze zbędnym okablowaniem

Funkcja Power over Ethernet (PoE) pozwala na zasilanie i połączenie sieciowe poprzez port LAN za pośrednictwem jednego kabla sieciowego. Skorzystanie z rozwiązania PoE redukuje liczbę potrzebnego okablowania znacznie redukując koszty związane z zakupem kabli do urządzeń sieciowych, a także umożliwia zamontowanie urządzenia w miejscu, gdzie niemożliwa byłaby instalacja źródła zasilania.

Standard szyfrowania: **WPA3**

Standard WiFi: **802.11ax (gen.6)**

Tryb pracy: **Access point**

Zastosowanie: **Wewnętrzne**

9 Wideodomofon

Budynek wyposażony jest w system wideo domofonowy. System składa się z następujących elementów:

- panele wywoławcze z funkcją wideo (brama, wejścia główne)
- panele odbiorcze z funkcją wideo (Pom. stałego dozoru, zespół pomieszczeń kancelarii tajnej)

Domofon wyposażony jest również w funkcję interkomu który umożliwia połączenie pomiędzy dowolnymi użytkownikami instalacji domofonowej.

Schemat i rozmieszczenie instalacji został pokazany na zamieszczonych rzutach.

System składa się z następujących elementów:

Centrałka sterująca

Rodzaj obudowy	DIN-6M
Pobór prądu średnio	70 mA
Montaż	Szyna DIN 35 x 7,5 x 1mm lub kołki rozstaw 75mm
Zasilanie	18V/1A(19V/3,15A), impulsowy zasilacz stabilizowany w zestawie
Zakres temperatur pracy	0 ... +40 °C
Połączenia wyprowadzeń sterowania	Rozłączalne listwy zaciskowe, raster 3,5mm
Wyprowadzenia sygnału wizji	BNC 75 ohm
Wejście przycisku otwarcia drzwi	Tak
Współpraca z systemem pożarowym SAP	Tak, poprzez programowalne, wielofunkcyjne wejście DR
Regulacje	Poziomy sygnałów w obu kierunkach transmisji, równoważenie toru rozmównego
Prędkość transmisji między modułami	2400, 4800, 9600 baud
Zaczep rewersyjny	Maksymalny pobór prądu 250 mA
Gniazdo magistrali komutacji pionowej	RJ45
Masa	210 g

Zasilacz 18V, 1A

Moduł komutacji

Komutator służy do rozdzielenia sygnału na cztery stacje wywoławcze

Rodzaj obudowy	płaska, materiał ABS
Montaż	naścienny, kołki rozstaw 57 mm (średnica łba 7-8mm)
Gniazda łączeniowe	linie rozmówne - gniazda RJ-12, magistrala - RJ-45
Zasilanie	z linii lub dodatkowy zasilacz 18V/1A
Pobór prądu	0,9 mA
Zakres temperatur pracy	0 ... +40 °C
Masa	50 g

Moduły odbiorcze

Stacja odbiorcza jest montowana naściennie nie wymaga wykuvania otworów w ścianie.

Podstawowe cechy to:

- Kolorowy obraz, ekran TFT-LCD 3,5"
- Podgląd z kamery lokalnej
- Łączność z portierem
- Regulacja głośności sygnału zewu
- Regulacja jaskrawości i nasycenia barw obrazu
- Otwieranie drzwi (uruchamianie zaczepu elektrycznego w drzwiach - opcja)
- Brak przewodów koncentrycznych. Instalacja przewodem UTP kat.5
- Funkcja zastępcza dzwonka do drzwi

Monitor wyposażony jest w odłączalną ramkę umożliwiającą zamocowanie jej na ścianie a następnie zamocowanie na niej monitora.

Wielkość ekranu	TFT-LCD 3,5" kolorowy
Pobór prądu w stanie spoczynkowym	3,5 mA
Pobór prądu w stanie pracy	280 mA
Napięcie zasilania	18V z linii domofonowej
Rozdzielczość ekranu	480 x 234
Klawiatura	3 przyciski funkcyjne
Komunikacja audio	Full duplex, rozłączalny mikrotelefon
Regulacja parametrów	głośność zewu, jasność, nasycenie barw
Funkcja OSD	nie
Funkcja dzwonka zastępczego	tak
Ilość żył kabla sygnałowego	6
Rodzaj kabla	UTP kat. 5e 4x2x0.5
Sposób łączenia kabla	rozłączalna listwa zaciskowa
Wylłącznik monitora	tak
Wymiary monitora	Szerokość : 255mm, wysokość : 125mm, głębokość : 35mm (bez słuchawki)

Moduł wywoławczy:

Zawiera kamerę kolorową, odbiornik pilota radiowego, klawiaturę zbliżeniową oraz skaner linii papilarnych lub czytnik kart RFID. Wyposażony jest w kamerę WDR z konfigurowalnym MENU.

- kolorowy obraz w systemie (dla wersji wideo), obudowa modułu wykonana jako wtrysk stopu aluminium
- podświetlenie podczerwieni (opcja), obracana w poziomie kamera za szybą z poliwęglanu
- graficzny wyświetlacz LCD widoczny w dzień i w nocy !
- zbliżeniowa, świecąca klawiatura niewrażliwa na warunki atmosferyczne i zabrudzenia
- wbudowana obsługa listy lokatorów wydzielone przyciski funkcyjne
- skaner linii papilarnych lub czytnik RFID . (*)
- instalacja prowadzona płaskim 6-żyłowym kablem telefonicznym lub UTP
- komutowane w systemie indywidualne linie rozmówne !
- możliwość łączenia w system wielu budynków
- możliwość przekierowania połączeń do innego lokalu
- łączność z portierem
- łączność z dowolnej bramy wejściowej z dowolnym aparatem
- obsługa obiektów o wielu wejściach
- otwieranie drzwi lub bramy kodem ogólnym lub indywidualnym
- otwieranie drzwi lub bramy za pomocą pilota radiowego
- otwieranie drzwi lub bramy za pomocą skanu linii papilarnych (*)
- otwieranie drzwi lub bramy za pomocą czytnika kart RFID (*)
- programowanie przez użytkownika jego własnego kodu
- możliwość zdalnego otwierania aparatem bramy wjazdowej
- niewrażliwość systemu na zwarcie dowolnej linii rozmównej
- konfiguracja parametrów roboczych systemu za pomocą zewnętrznego komputera !!
- możliwość rejestracji wszystkich zdarzeń (wejść, użycia kodów itp.) na zewnętrznym komputerze
- kod bezpieczeństwa uniemożliwiający uruchomienie modułu zewnętrznego po kradzieży
- archanielska słyszalność (stała czasowo i praktycznie niezależna od wielkości systemu)
- automatyczna samokontrola systemu

Opis działania:

Panel wywoławczy zostanie umieszczony przy wejściach głównych, bramach i wejściu do zespołu kancelarii tajnej KT. Za pomocą panelu wywoławczego możliwe jest połączenie z każdym modulem odbiorczym w budynku.

Użytkownik może wejść do środka poprzez zezwolenie ze stacji odbiorczej, wpisanie kodu lub przyłożenie karty dostępu.

Otwarcie odbywa się poprzez system kontroli dostępu co umożliwia rejestrację zdarzeń.

Dodatkowo będzie możliwość podłączenia przenośnych telefonów, który umożliwią odebranie sygnału z domofonu.



10 Instalacja przyzywowa

Budynek wyposażony jest w instalację przyzywową, zlokalizowaną w pomieszczeniach toalet z funkcją dla osób niepełnosprawnych. Instalacja składa się z następujących elementów:

- panel sali zamocowany w przedsionku do toalety,
- lampa sygnalizacyjna przed wejściem do toalety
- przycisk łazienkowy – działanie przez pociągnięcie
- zasilacz 12V/8A

Pociągnięcie przycisku w łazience spowoduje załączenie lampki przed wejściem do łazienki, i pomieszczeniu portiera. Skasowanie alarmu następuje poprzez wciśnięcie przycisku na panelu sali.

Schemat i rozmieszczenie instalacji został pokazany na zamieszczonych rzutach.

11 BMS

Projekt zakłada wykonanie instalacji do systemu BMS.

Budynek wyposażony będzie w instalację BMS która będzie sterowała następującymi elementami instalacji:

- ☐ Sterownie klimatyzacją
- ☐ Sterowanie wentylacją
- ☐ Odczyt danych z liczników: analizatora sieci elektrycznej, licznik ciepła, licznik wody zimnej i ciepłej
- ☐ Nadzorowanie instalacji fotowoltaicznej
- ☐ Nadzorowanie instalacji kontroli dostępu KD

- ☐ Nadzorowanie instalacji alarmowej SSWiN1 i SSWiN2
- ☐ Nadzorowanie instalacji CCTV
- ☐ Nadzorowanie instalacji Monitoringu AW
- ☐ Nadzorowanie instalacji SSP
- ☐ Nadzorowanie instalacji DSO
- ☐ Nadzorowanie i sterowanie instalacją oświetlenia ogólnego
- ☐ Nadzorowanie i sterowanie instalacją oświetlenia zewnętrznego
- ☐ Nadzorowanie instalacji przyzywowej
- ☐ Nadzorowanie instalacji UPS
- ☐ Sterowni i nadzorowanie pompą ciepła
- ☐ Sterowni i nadzorowanie szafą klimatyzacji precyzyjnej
- ☐ Sterowni i nadzorowanie klimatyzatorami w pomieszczeniach w zależności od otwarcia okien i ogrzewania (patrz punkt 8)
- ☐ Odczyt danych z tablic elektrycznych (ochronniki, czujniki zaniku fazy)
- ☐ Załączanie wentylatorów dachowych
- ☐ Sterowanie grzałką elektryczną w podgrzewaczu c.w.u.

Głównym elementem systemu jest sterownik z budowanym Web-Serverem. Wszystkie elementy systemu będą komunikować się za pomocą sieci BACnet IP. Wyjątkiem są liczniki energii, analizator sieci elektrycznej, czujniki temperatury w pomieszczeniach i klimatyzatory które będą komunikować się po sieci Modbus RTU.

Centrale wentylacyjne

System BMS będzie realizował następujące funkcję udostępnione przez producenta:

- Monitorowanie i sterowanie parametrami pracy zainstalowanych w ww. obiekcie urządzeń oraz zobrazowanie aktualnego stanu w jakim się znajdują, wraz z monitorowaniem parametrów pracy (temperatury, ciśnienie, wysterowania, przepływy itp.).
- Sygnalizowanie alarmowe przekroczenia parametrów zadanych.
- Sygnalizowanie alarmów urządzeń.
- Możliwość sterowania ręcznego.
- Sygnalizowanie alarmowe wyłączenia z uwagi na sygnał pożarowy z systemu SSP
- Użycie harmonogramów czasowych oraz trybów pracy umożliwiających wybór nastaw pracy dziennych i nocnych.
- Pomiar stężenia CO₂ w kanale wyciągowym.
- Sterowanie i monitorowanie w BMS układu dostarczającego chłód do centrali (np. agregatu WL/agregatu freonowego - w zależności od zastosowanego w projekcie sanitarnym).
- Sterowanie i monitorowanie wentylatorów wyciągowych
- Do urządzeń wykonawczych takich jak siłowniki zaworów zaprojektować sygnał zwrotny położenia zaworu.

Agregat wody lodowej

Poniżej zestaw możliwych funkcjonalności poprzez BMS:

- zarządzanie elektronicznym zaworem rozprężnym,
- zarządzanie przedziałami czasowymi i parametrami roboczymi z możliwością tygodniowego/dziennego programowania działania,
- zarządzanie zdalną wartością zadaną za pomocą temperatury zewnętrznego powietrza (krzywa klimatyczna); regulacja temperatury wody na wlocie do maszyny,
- zarządzanie pompą obiegową z funkcją „pump energy saving”,
- ochrona przed zamarzaniem z automatyczną aktywacją w stanie czuwania,
- czasowe funkcje bezpieczeństwa,
- czasowe funkcje sprężarek,
- reset alarmów,
- zarządzanie alarmami i diodami LED działania,
- lokalne lub zdalne przełączanie cyklu chłodzenia/ogrzewania.
- Wyświetlanie: - cyklu pracy (chłodzenie/ogrzewanie/wytwarzanie ciepłej wody użytkowej, odszranianie),
- temperatura wody na wlocie/wylocie,
- temperatura zadana i ustawiona różnica temperatur,
- kod i wyświetlanie alarmów, które się włączyły.

Pompa ciepła

Poniżej zestaw możliwych funkcjonalności poprzez BMS:

1. Start/stop (nastawa)
2. Start/stop (stan bieżący)
3. Kod usterki – kod błędu
4. Alarm
5. Tryb pracy klimatyzatora (Nastawa)
6. Tryb klimatyzacji (Ustawienia grzanie/ chłodzenie)
7. Tryb klimatyzacji (Stan bieżący grzanie / chłodzenie)
8. Poziom natężenia przepływu powietrza (Stan bieżący)
9. Pomiar temperatury pomieszczenia (Stan bieżący)
10. Ustawia temperaturę pomieszczenia (Nastawa)
11. Sygnał znaku zabrudzenia filtra (Stan bieżący) – ustawienie czasowe
12. Resetowanie sygnału znaku filtra
13. Zdalne włączanie / wyłączanie (start / stop)
14. Zdalne włączanie / wyłączanie (tryb klimatyzacji grzanie/ chłodzenie)
15. Pilot zdalnego sterowania włącza / wyłącza (ustawia temperaturę)
16. Pobór mocy elektrycznej - monitoring
17. Status komunikacji (ok/błąd)
18. Wymuszenie zatrzymania systemu
19. Kierunek powietrza (nastawa) - jeśli dostępne w jednostce wewnętrznej
20. Kierunek powietrza (stan) - jeśli dostępne w jednostce wewnętrznej
21. Oszczędzanie zużycia energii (nastawa)
22. Oszczędność zużycia energii (stan bieżący)
23. Stan pracy sprężarki
24. Stan wentylatora jednostki wewnętrznej (monitorowanie)
25. Stan pracy nagrzewnicy - opcjonalnie.

Sterowanie klimatyzacji

Poniżej zestaw możliwych funkcjonalności poprzez BMS:

1. Przełącza działanie ON / OFF i monitoruje stan pracy.
2. Monitoruje jednostki wewnętrzne pod kątem usterek. Sygnał awarii.
3. Monitoruje i zmienia nastawę temperatury w pomieszczeniu.
4. Monitoruje temperaturę jednostki wewnętrznej.
5. Monitoruje i resetuje sygnał zabrudzenia filtra - opcjonalnie.
6. Przełącza tryb pracy . (chłodzenie / grzanie)
7. ustawia funkcje na sterowniku.

UWAGA:

Bramka BACnet posiada dedykowane wejście dla instalacji SSP, które wyłącza całą klimatyzację w przypadku pożaru.

Węzeł cieplny (opcja)

Wytyczne do BMS:

- monitoring pomp ma uwzględniać przynajmniej monitoring sygnału pracy i awarii,
- w przypadku zastosowania pomp podwójnych na obiegach należy zaprogramować rozwiązanie automatycznego przełączania pomp w przypadku awarii, wyrównywanie czasu pracy pomp (okresowe przełączanie), funkcje okresowego uruchomienia,
- zabezpieczenie pomp przed suchobiegiem,
- zabezpieczenie przed przegrzaniem (stany termostatów STW i STB),
- siłownik zaworu musi umożliwiać odczytanie w BMS faktycznej pozycji zaworu, a nie tylko wartości polecenia sterującego (zaprojektować sygnał zwrotny położenia siłowników);
- monitoring parametrów dla obiegów: temperatura zasilania, temperatura powrotu, ciśnienie zasilania, ciśnienie powrotu;

Wymagania stacji zarządzania

Wszystkie informacje przesyłane są do poziomu zarządzania. Poziom zarządzania to graficzny, interaktywny interfejs dla operatora do sterowników wraz z zintegrowanymi instalacjami i ich komponentami.

Stacja zarządzania jest oparta o architekturę serwer-klient i musi zapewniać obsługę następujących funkcji:

- Prezentowanie instalacji w formie graficznych synoptyk, z wartościami i stanami wyświetlanymi statycznie i dynamicznie.
- Możliwość importu rzutów i symboli CAD - .DWG .DXF (import formatów AutoCaD do wersji 2012 włącznie)
- Obsługa warstw stworzonych grafik w systemie BMS, na przykład w celu prezentacji różnych instalacji grupami urządzeń na rzucie piętra
- Wizualizację i obsługę alarmów
- Filtrowanie alarmów według atrybutów lub priorytetów alarmów.
- Bezpośrednią nawigację od elementu wyzwalającego zdarzenie na grafikę systemu.
- Log zdarzeń
- Możliwość konfiguracji dystrybucji alarmów na drukarkę, e-mail, SMS
- Edycję i tworzenie raportów.
- Raporty z możliwością drukowania lub exportu do formatu PDF, .csv

- Wyświetlanie wieloprzebiegowych trendów (do 10 wartości na widok trendu), z opcją porównywania danych trendów w przesunięciu czasowym
- Dostęp do urządzeń w sieci BACnet;
- Zarządzanie układami regulacji i sterowania;
- Zarządzanie użytkownikami i grupami z dostępem do praw zapisu / odczytu, konfigurowania widoczności alarmów i instalacji według rodzaju (grupy) użytkownika, dostępu do zaawansowanych i podstawowych funkcji obsługowych;
- Możliwość wykonywania reakcji w celu automatyzacji czynności użytkownika, np. cykliczne generowanie raportów, generowanie raportów w przypadku wystąpienia zdarzenia,
- Możliwość wykonywania funkcji logicznych takie jak makra, skrypty- możliwość konfigurowania przez użytkownika działań na grupowanych obiektach systemu, w postaci makr, wywoływanych z przycisku na grafikach lub czasowo lub zdarzeniowo wykonywanych reakcji (np. do resetowania temperatur zadanych, podwyższenia lub obniżenia temperatury).,
- W celu archiwizacji i magazynowania danych system zapisuje dane w historycznej bazie danych,
- W bazie historycznej system może przechowywać następujące dane: działania użytkownika w systemie, alarmy i reakcje na nie, wartości zarejestrowane w trendach
- Stacja zarządzania BMS musi wspierać obsługę systemów rozproszonych (distributed systems) w topologii hierarchicznej, sieciowej i segmentowej,
- Stacja BMS musi mieć możliwość integracji zewnętrznych systemów informatycznych oraz aplikacji dostawców zewnętrznych z wykorzystaniem powszechnie stosowanego, otwartego interfejsu REST API,
- Stacja BMS musi mieć możliwość implementacji na stacji BMS skryptów wykonujących dowolnie zaprogramowany algorytm w powszechnie wykorzystywanym języku JavaScript

Wielu użytkowników ma możliwość jednoczesnej pracy z systemem na wielu poziomach systemu automatyki i zarządzania budynkiem w celu efektywnej pracy.

System automatyki musi oferować możliwość podglądu i zarządzania zdalnego systemem BMS z poziomu najbardziej popularnych przeglądarek internetowych (Chrome, Safari, Firefox) oraz urządzeniach z systemami operacyjnymi Microsoft Windows, MacOS, iOS, Android dzięki technologii HTML5. Synoptyki systemu muszą dawać możliwość komfortowej obsługi systemu zarówno z wykorzystaniem myszki i klawiatury jak i ekranów dotykowych.

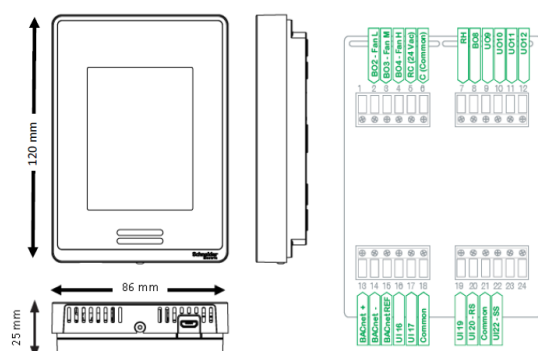
Sterowanie klimatyzacją i ogrzewaniem

W pomieszczeniach z klimatyzatorami, zostaną zainstalowane regulatory temperatury sterujące zaworami grzejnikowymi 24VAC. regulatory i klimatyzatory zostaną połączone ze sterownikiem BMS przewodem ModBus według załączonych schematów.

Klimatyzatory muszą być zgodne z protokołem Modbus (RS485)

Regulator:

Wymiary



Specyfikacja

Element	Opis
Wymiary	120 mm (wys.) x 86 mm (szer.) x 25 mm (gł.)
Zasilanie	24 V AC $\pm 15\%$, 50/60Hz 24 do 28 V AC 50/60 Hz (z modułem czujnika CO ₂), 12 VA Maksymalna moc znamionowa transformatora: 100 VA, 4,17 A
Obciążalność prądowa wyjść	Wyjścia przekaźnikowe: 28 V AC 50/60 Hz, 1,0 A, krótkotrwały = 3,0 A; wyprowadzenia 1, 2, 3, 4, 5, 8, 9 Wyjścia optomos: 28 V AC 50/60 Hz, 0,3 A, krótkotrwały = 1,5 A; wyprowadzenia 9, 10, 11, 12 Wyjścia analogowe: 0–10 V DC przy min. obciążeniu 2 k Ω (do 5 mA); wyprowadzenia 9, 10, 11, 12
Wejścia analogowe	Wejścia analogowe UI19 do UI24: 0-10 V DC
Wejście binarne	Styki bezpotencjałowe UI16, UI17
Wymagania zewnętrznego czujnika temperatury	Termistor 10K NTC typu 2 UI20, UI22, UI23
Warunki pracy	0°C do 50°C Wilg. wzgl. 0% do 75% bez kondensacji
Warunki przechowywania	-30°C do 50°C Wilg. wzgl. 0% do 75% bez kondensacji
Czujnik temperatury	Lokalny termistor 10K NTC typu 2
Czułość czujnika temperatury	0,1°C
Dokładność pomiaru temperatury	Skalibrowana typowo 0,5°C dla 21°C
Czujnik wilgotności i kalibracja	Jednopunktowy, skalibrowany czujnik polimerowy
Precyzja czujnika wilgotności	Zakres odczytu wilg. wzgl. 10 do 90%, bez kondensacji; W zakresie 10% do 20% - precyzja 10% W zakresie 20% do 70% - precyzja 5% W zakresie 70% do 90% - precyzja 10%
Stabilność czujnika wilgotności	Poniżej 0,25% w ciągu roku
Zakres nastawy osuszania	Wilg. wzgl. 30% do 95%
Zakres nastawy chłodzenia	12°C do 37,5°C
Zakres nastawy grzania	4,5°C do 32°C
Zakres wyświetlania temperatury	-40°C do 50°C
Martwa strefa sterowania temperaturą	domyślnie: 1,8°C
Przekrój żyły	Zasilanie: 0,823 mm ² lub więcej Komunikacja MSTP: 0,205 mm ² lub więcej
Waga z opakowaniem	0,34 kg

Zastosowania:

- Systemy VAV
- Nagrzewnice
- Grzejniki
- Belki chłodzące
- Klimakonwektory dwu- i czterorurowe
- Inne

Sterowanie grzałką elektryczną w podgrzewaczu c.w.u.

Załączanie grzałki elektrycznej w podgrzewaczu c.w.u będzie wykonywane poprzez sterownik BMS umieszczony w rozdzielni głównej RG. Głównym zadaniem sterownika będzie uruchamianie podgrzewu wody użytkowej w sezonie letnim przy wykorzystaniu energii elektrycznej (pochodzącej z fotowoltaiki). Sterownik poprzez odpowiednie oprogramowanie, będzie zbierał informacje ze stacji pogodowej i włączał/wyłączał grzałkę w zależności od nasłonecznienia.

W przypadku wyłączenia przez sterownik grzania w podgrzewaczu, z systemu BMS zostanie przesłana informacja do automatyki kotła gazowego w celu załączenia pełnego podgrzewu.

W pomieszczeniu kotła gazowego należy zainstalować gniazdo elektryczne i podłączyć z podgrzewaczem na etapie wykonawczym.

Podgrzewacz musi być wyposażony w grzałkę elektryczną.

Serwer WWW

Serwer web umożliwia dostęp do systemu poprzez przeglądarkę internetową. Pozwala na pobranie wszystkich plików niezbędnych do działania klienta www oraz klienta aplikacji Windows. Zapewnia także systemową stronę www oferującą dostęp do klienta www, klienta aplikacji Windows i dokumentacji systemowej w przeglądarce internetowej. Reprezentuje także punkt końcowy komunikacji z serwerem systemowym.

Programy czasowe

Definicja harmonogramów umożliwia zmianę harmonogramów z poziomu stacji zarządzania w sterowniku budynkowym w celu zapewnienia czasowego sterowania pracą urządzeń nawet gdy serwer BMS jest wyłączony. Jako minimum należy obsługiwać następujące funkcje:

- Pełna obsługa wszystkich obiektów BACnet typu Scheduler, Calendar
- Harmonogramy dzienne i tygodniowe
- Obsługa kalendarza - wyjątki określone na podstawie lokalnego bądź globalnego kalendarza mają możliwość nadpisania tygodniowego programu czasowego dla instalacji.

Projektowane instalacje automatyki i BMS muszą być kompatybilne z ww. oprogramowaniem w celu bezproblemowej integracji i wizualizacji w założonej w projekcie funkcjonalności.

Zadaniem wykonawcy jest wykonanie wizualizacji na stacji BMS. Urządzenia należy wizualizować w sposób czytelny dla Użytkownika, z odniesieniem do lokalizacji na rzutach budynku, przy użyciu graficznych synoptyk.

Zadaniem Wykonawcy jest uwzględnienie całego zakresu niezbędnych usług, dostaw i prac do wykonania ww. wizualizacji, w tym uwzględnienie odpowiedniego rozszerzenia licencji serwera BMS.

Na Grafikach rzutów pięter wraz z urządzeniami należy pokazać najważniejsze parametry danego urządzenia (np. temperatura w pomieszczeniu, temperatura nawiewu/wyciągu natomiast dla central wentylacyjnych praca/awaria wentylatorów, ect.)

W systemie BMS należy skonfigurować trendy rejestrujące najważniejsze parametry pracy urządzeń oraz powietrza (wartości pomiarowe z pomieszczeń w zależności od zaprojektowanego rodzaju czujnika - temperatura / wilgotność / CO₂, w centralach wentylacyjnych temperatury nawiewu / wywiewu, ciśnienia,ysterowanie elementów grzewczych, chłodniczych ect.).

Fakt przeszkolenia obsługi technicznej z wprowadzonych do systemu BMS zmian należy potwierdzić protokołem szkolenia dołączonym do dokumentacji powykonawczej.

Kontrola jakości robót systemu BMS,

Wyszczególnienie robót:

Należy wykonać sprawdzenia odbiorcze składające się przede wszystkim z oględzin częściowych i końcowych polegających na kontroli:

- ☐ zgodności dokumentacji powykonawczej z projektem i ze stanem faktycznym,
- ☐ zgodności połączeń z podanymi w dokumentacji powykonawczej,
- ☐ stanu kanałów i listew kablowych, kabli i przewodów, osprzętu instalacyjnego do kabli i przewodów, stanu i kompletności dokumentacji dotyczącej zastosowanych materiałów,
- ☐ sprawdzenie ciągłości wszelkich przewodów występujących w danej instalacji,
- ☐ poprawności wykonania i zabezpieczenia połączeń śrubowych instalacji BMS potwierdzonych protokołem przez wykonawcę montażu,
- ☐ poprawności wykonania montażu sprzętu instalacyjnego, urządzeń i odbiorników energii elektrycznej,
- ☐ pomiarach rezystancji izolacji,
- ☐ napisów informacyjno-ostrzegawczych,
- ☐ działania przyrządów kontrolno-pomiarowych i rejestrujących (liczniki energii elektrycznej),
- ☐ działania sygnalizacji stanu położenia łączników,
- ☐ stanu i gotowości ruchowej aparatury i napędów łączników,
- ☐ stanu zewnętrznego głowic kablowych,
- ☐ stanu kanałów kablowych, kabli i konstrukcji wsporczych,
- ☐ stanu ochrony przeciwporażeniowej,
- ☐ stanu urządzeń wentylacyjnych - chłodzenie rozdzielnic,
- ☐ schematu stacji, rozdzielnic lub sterownicy,
- ☐ stanu i kompletności dokumentacji eksploatacyjnej,
- ☐ sprawdzenie ciągłości przewodów fazowych, neutralnych i ochronnych,
- ☐ poprawności wykonania połączeń śrubowych instalacji BMS potwierdzonych protokołem przez wykonawcę montażu.
- ☐ Dla układów sterowniczo-sygnalizacyjno-pomiarowych sprawdzenia odbiorcze polegają na:
 - ☐ pomiarach rezystancji izolacji,
 - ☐ sprawdzeniach funkcjonalnych, ruchowych i nastawczych,
 - ☐ zbadaniu przyrządów kontrolno-pomiarowych i rejestrujących (analizatory sieci),
 - ☐ zbadaniu wartości nastawczych wyłączników, przekaźników termicznych, przekaźników różnicowo prądowych, itp. Rezystancja izolacji obwodów nie powinna być mniejsza niż 50 MΩ. Rezystancja izolacji poszczególnych obwodów wraz z urządzeniami nie powinna być mniejsza niż 20 MΩ. Pomiaru należy dokonać miernikiem rezystancji instalacji o napięciu 1 kV.
- ☐ Prawidłowości działania centralnego systemu nadzoru po aktualizacji oprogramowania i uzupełnienia elementów wizualizacji systemu.

Po wykonaniu oględzin należy sporządzić protokoły z przeprowadzonych badań.

Wszystkie materiały, urządzenia i aparaty nie spełniające wymagań podanych w odpowiednich punktach specyfikacji, zostaną odrzucone. Jeśli materiały nie spełniające wymagań zostały wbudowane lub zastosowane, to na polecenie Inspektora nadzoru Wykonawca wymieni je na właściwe, na własny koszt.

Na pisemne wystąpienie Wykonawcy Inspektor nadzoru może uznać wadę za niemającą zasadniczego wpływu na jakość funkcjonowania instalacji i ustalić zakres i wielkość potrąceń za obniżoną jakość.

Należy stosować okablowanie w klasie reakcji: B2ca

Odbiór końcowy systemu BMS,

Wyszczególnienie robót:

Odbioru końcowego dokonuje komisja odbiorcza powołana przez inwestora.

Odbiór końcowy instalacji BMS obejmuje:

- ☐ sprawdzenie przedstawionych dokumentów - dokumentacji powykonawczej,
- ☐ sprawdzenie zgodności wykonanej instalacji z umową, warunkami przyłączenia do sieci elektroenergetycznej, projektem instalacji, przepisami techniczno- budowlanymi, Polskimi Normami oraz zasadami wiedzy technicznej,
- ☐ oględziny instalacji,
- ☐ sprawdzenie skuteczności działania zabezpieczeń i środków ochrony przed porażeniem prądem elektrycznym,
- ☐ przeprowadzenie badań i prób montażowych,
- ☐ przeprowadzenie prób rozruchowych,
- ☐ sporządzenie protokołu odbioru.

12 Kanalizacja teletechniczna

Na potrzeby przyłącza telekomunikacyjnego wykonany zostanie element kanalizacji teletechnicznej składającej się z rury RHDPEp 110/6,3 oraz studzienek SKR-1. Rzut przyłącza pokazany został na planie zagospodarowania terenu.

Opis wykonania przyłącza

Teletechniczną kanalizację kablową z rur cienko ściennych o grubości ścianki od 3 do 5mm wykonujemy w miejscach o małym zagrożeniu uszkodzeniami mechanicznymi, natomiast z rur grubościennych o podwyższonej wytrzymałości, grubości ścianki nie mniejszej niż 5mm wykonujemy w miejscach szczególnie obciążonych, np: w pasie rozdzielającym jezdnie, pod jezdniami, pod placami, pod torowiskami, w pasie drogowym.

Kanalizację , należy budować z rur z polietylenu RHDPE 110/6,3.

Kanalizację kablową , należy układać na wyrównanym i ubitym podłożu pozbawionym kamieni i korzeni, a w przypadku gruntów mało spoistych na wylanej ławie z betonu marki 100 o grubości min. 0,1m. Rury należy układać warstwami zasypując piaskiem lub przesianą ziemią lekko ubijając i przelewając wodą . Ostatnią warstwę rur należy przysypać warstwą piasku lub przesianej ziemi o grubości min.

0,05m, a następnie warstwą piasku lub przesianej ziemi o grubości, co najmniej 0,2m i kolejnymi warstwami ziemi po 0,2m ubijanymi mechanicznie zagęszczając grunt do wartości uzgodnionej z właścicielem pasa drogowego. Rury kanalizacji kablowej, należy łączyć przy pomocy złączy rurowych, zgodnie z instrukcją

przewidzianą przez producenta. Głębokość ułożenia kanalizacji teletechnicznej w ziemi mierzona od powierzchni ziemi do górnej powierzchni kanalizacji winna wynosić nie mniej niż :

0,6m - w przypadku kanalizacji ułożonej poza pasem drogowym,

0,6m - w przypadku kanalizacji ułożonej w pasie drogowym,

W szczególnych przypadkach uzasadnionych trudnościami technicznymi dopuszcza się zmniejszenie głębokości ułożenia kanalizacji za zgodą właściciela terenu, pod warunkiem jej odpowiedniego zabezpieczenia rur np. ławą betonową , lub wykonania kanalizacji rur stalowych bądź z rur z tworzywa sztucznego o podwyższonej wytrzymałości. Długość przęsła kanalizacji teletechnicznej magistralnej nie powinna przekraczać 120m.

Przy budowie telekomunikacyjnej kanalizacji kablowej, należy zachować właściwe odległości od innych urządzeń podziemnych zgodnie z ZN-96 TPSA - 004.

Wytyczne wynikające z warunków przyłączenia:

- jednootworowe przyłącze projektowanego budynku z nawiązaniem do studni teletechnicznej Orange Polska S.A zlokalizowanej przy ul. Bartniaka, oznaczonej w Orange: GRODZISK MAZ/OST/01753 (załącznik z lokalizacją studni).
- projektowane przyłącze budować jako kanalizację kablową z rur PCW 110, bądź jako rurociąg kablowy z rur HDPE 40/3,7 z pilotem,
- przejścia pod drogami i miejscami parkingowymi zaprojektować z rur RHDPEp 110/6,3
- w ciągu projektowanej kanalizacji pierwotnej zastosować studnie kablowe typu SKR-1
- studnie kablowe projektować wyposażone w pokrywy zewnętrzne, z układem zasuwowo-ryglowym, blokowanym zamkiem typu Abloy oraz przystosowane do zamontowania czujników systemu elektronicznego monitorowania elementów sieci,
- wejścia projektowanej kanalizacji PCW do budynku i studni, należy zabezpieczyć dwustronnie (od strony budynku i od strony studni) z wykorzystaniem zestawów uszczelniających.

13 Warunki techniczne przyłączenia do sieci teletechnicznej



Orange Polska
Hurt
Infrastruktura i Serwis Usług
Dział Zarządzanie Zasobami Infrastruktury i Obsługi Klienta
ul. Aleje Jerozolimskie 160, 02-326 Warszawa
tel.: +48 501 328 572

Skarb Państwa
Prokuratura Okręgowa w Warszawie
ul. Chocimska 28
00-791 Warszawa

Warszawa, 7 lutego 2023

Numer pisma: 2512/TTDSILU/P/2023/BS

Temat: techniczne warunki nawiązania do sieci telekomunikacyjnej Orange Polska S.A. projektowanego budynku Prokuratury Rejonowej zlokalizowanego przy ul. Bartniaka w Grodzisku Mazowieckim dz. nr ew. 11/5 obręb 0029.

Szanowni Państwo,

W odpowiedzi na Państwa wniosek informujemy, że celem nawiązania w/w obiektu do sieci telekomunikacyjnej należy zaprojektować:

- jednootworowe przyłącze projektowanego budynku z nawiązaniem do studni teletechnicznej Orange Polska S.A. zlokalizowanej przy ul. Bartniaka, oznaczonej w Orange: GRODZISK MAZ/OST/01753 (załącznik z lokalizacją studni).
- projektowane przyłącze budować jako kanalizację kablową z rur PCW 110, bądź jako rurociąg kablowy z rur HDPE 40/3,7 z pilotem,
- przejścia pod drogami i miejscami parkingowymi zaprojektować z rur RHDPE 110/6,3
- w ciągu projektowanej kanalizacji pierwotnej zastosować studnie kablowe typu SKR-1
- studnie kablowe projektować wyposażone w pokrywy zewnętrzne, z układem zasuwowo-ryglowym, blokowanym zamkiem typu Abloy oraz przystosowane do zamontowania czujników systemu elektronicznego monitorowania elementów sieci,
- wejścia projektowanej kanalizacji PCW do budynku i studni, należy zabezpieczyć dwustronnie (od strony budynku i od strony studni) z wykorzystaniem zestawów uszczelniających.

Niniejsze warunki wydaje się dla celów projektowych i nie stanowią one zobowiązania Orange Polska S.A. do wykonania przyłączenia do sieci telekomunikacyjnej. Przyłączenie do sieci telekomunikacyjnej może być zrealizowane wyłącznie na podstawie wcześniej zawartej umowy o świadczenie usług przez Orange Polska S.A.

Jeżeli inwestor zainteresowany jest korzystaniem z usług Orange Polska S.A., to informację w tej sprawie może uzyskać poprzez zakładkę **Kontakt** na stronach:

<https://www.orange.pl/duze-firmy> lub

<https://www.orange.pl/male-srednie-firmy>

Orange Polska Spółka Akcyjna z siedzibą i adresem w Warszawie (02-326) przy Al. Jerozolimskich 160, wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem 000010601; REGON 012100704, NIP 526-02-50-965, z pokrytym w całości kapitałem zakładowym wynoszącym 3.807.072.437 złotych.

W przypadku realizacji prac projektowych przez Klienta należy projektowane trasy i lokalizacje urządzeń telekomunikacyjnych uzgodnić zgodnie z obowiązującymi przepisami prawa, a następnie wraz z projektem wykonawczym złożyć do uzgodnienia i zatwierdzenia przez Infrastruktura i Serwis Usług, Dział Zarządzania Zasobami Infrastruktury i Obsługi Klienta, ul. Aleje Jerozolimskie 160, 02-326 Warszawa, lub w formie elektronicznej na adres e-mail: ZZSS.przebudowa.infrastruktury.lodz@orange.com

Warunki korzystania z kanalizacji teletechnicznej Orange Polska S.A. uregulowane zostaną w odrębnej umowie.

Szczegółowe dane techniczne zostaną udzielone w Dziale Zarządzania Zasobami Infrastruktury i Obsługi Klienta – w siedzibie ul. Aleje Jerozolimskie 160 w Warszawie (sprawę prowadzi: Bogdan Sadowski, tel. 501 328 572) lub poprzez e-mail: ZZSS.przebudowa.infrastruktury.lodz@orange.com.

Wewnętrzne instalacje telefoniczne w planowanych obiektach, zgodnie z Rozporządzeniem Ministra Infrastruktury z dnia 12.04.2002 r. (Dz.U. 2002 nr 75 poz. 690) z późniejszymi zmianami, należy wybudować w ramach własnej inwestycji. Sieć wewnętrzna, powinna być sprowadzona do punktu styku z zaprojektowanym przyłączem zewnętrznym. Musi spełniać przepisy techniczno - budowlane i wymagania UKE, dotyczące minimalnej przepływności łączy. Należy ją zrealizować z zastosowaniem kabli teleinformatycznych.

Przed rozpoczęciem prac przy i na urządzeniach telekomunikacyjnych Inwestor ma obowiązek wystąpić, co najmniej 14 dni przed planowanym rozpoczęciem robót, z wnioskiem w celu zlecenia świadczenia nadzoru w trakcie prac wykonywanych na sieci i na urządzeniach telekomunikacyjnych ORANGE POLSKA. Wniosek dostępny jest na stronie www.orange.pl/wniosek nadzor. Po wypełnieniu wszystkich wymaganych pól wniosek zostanie automatycznie przesłany i zarejestrowany przez Orange Polska S.A. Istnieje również możliwość przesłania wniosku w postaci papierowej do Orange Polska S.A. Obsługa Techniczna Klienta i Infrastruktury:

Orange Polska S.A
Techniczna Obsługa Klienta i Infrastruktury
Obsługa Techniczna Klienta Centrum
ul. Piękna 19b, 00-549 Warszawa
e-mail: DISU.RC.Korespondencja@orange.com

UWAGA:

Informujemy, że w obszarze działań inwestycyjnych mogą znajdować się elementy infrastruktury telekomunikacyjnej (kable szafy, puszki) będące pod napięciem niebezpiecznym. Elementy te oznaczone są przywieszkami koloru czerwonego, zawierającymi informację o występowaniu napięcia niebezpiecznego. W dokumentacji projektowej należy umieścić Informację o możliwości występowania na trasie/w relacji projektowanego zasobu, elementów infrastruktury z napięciami niebezpiecznymi i konieczności zachowania szczególnych środków ostrożności podczas pracy na/w zbliżeniu z nimi.

Osoby przystępujące do wykonywania prac na tak oznakowanych elementach infrastruktury w których występują napięcia niebezpieczne, powinny posiadać aktualne uprawnienia SEP (E) oraz zobowiązane są do przestrzegania Instrukcji BHP.

Wykonawca przystępując do prac na infrastrukturze Orange Polska S.A., zobowiązany jest do przestrzegania i stosowania standardów w zakresie bezpieczeństwa i kontroli dostępu w zakresie:

- uzgodnienia terminu rozpoczęcia prac,
- prowadzenia prac wyłącznie pod nadzorem właścicielskim ze strony OPL,
- oznaczania miejsca prowadzenia prac tablicą informacyjną.

Szczegółowy sposób postępowania dla powyższych wymagań został zapisany na stronie:
www.orange.pl/wniosek nadzor.

Dla robót realizowanych na infrastrukturze telekomunikacyjnej będącej w użytkowaniu OPL należy spełnić wymóg znakowania miejsca prowadzenia prac tablicą informacyjną.

a. tablica informacyjna przekazywana jest przez przedstawiciela OPL:

- przedstawicielowi inwestora (wykonawcy) na etapie przekazania placu budowy lub,
- przedstawicielowi inwestora (wykonawcy) na etapie rozpoczęcia świadczenia nadzoru nad realizowanymi robotami, dla przypadku gdy realizowane prace nie wymagają przekazania placu budowy.

b. przedstawiciel inwestora zgłasza zamiar prowadzenia prac wysyłając wniosek poprzez stronę www lub na wskazany wydanych Warunków Technicznych adres Obsługi Techniczna Klienta uzupełniając przekazywany zakres informacji o dane dotyczące:

- miejsca prowadzenia prac,
- terminu rozpoczęcia i zakończenia prac,
- nazwiska i numeru telefonu do kierownika robót,

c. w odpowiedzi na złożony wniosek/zamiar rozpoczęcia robót/ przedstawiciel Inwestora (wykonawcy) otrzymuje od komórki Orange Polska, do której kierowany był wniosek (Obsługa Techniczna Klienta) numer zgłoszenia, pod którym wniosek został zarejestrowany,

d. wykonawca robót uzupełnia tablicę informacyjną (zgodnie z określonym standardem tj: dane uzupełniane dużymi literami, w sposób trwały, pisakiem koloru czarnego, ścieralnym) wprowadzając następujące dane:

- nazwę firmy - wykonawcę, lub podwykonawcę prac,
- imię nazwisko kierownika robót,
- numer telefonu komórkowego do kierownika robót,
- numer zgłoszenia, pod którym wniosek został zarejestrowany,

e. wykonawca uzupełnia zapisy na tablicy informacyjnej i umieszcza ją w widocznym miejscu np.: na zastawach ochronnych lub za przednią szybą od strony kierowcy w samochodzie wykonawcy znajdującym się na miejscu/w pobliżu wykonywanych prac,

f. po zakończeniu prac oraz usunięciu wprowadzonych zapisów, tablica informacyjna podlega zwrotowi do Orange Polska. Sposób zwrotu tablicy informacyjnej należy uzgodnić z przedstawicielem Orange Polska w momencie przekazania tablicy.

Niniejsze warunki są ważne przez okres sześciu miesięcy od daty wydania.

Orange Polska nie bierze odpowiedzialności za wszelkie działania Inwestora podjęte w związku z przedmiotową inwestycją.

Z poważaniem

Bogdan Sadowski



Główny Specjalista



Zarządzanie Zasobami Infrastruktury i Obsługi Klienta

II. Część rysunkowa

III. Dokumenty formalno-prawne

1 Oświadczenie Projektantów

Zgodnie z art. 34 ust. 3d pkt. 3 ustawy Prawo Budowlane oświadczam, że projekt wykonawczy dla budowy siedziby Prokuratury Rejonowej w Grodzisku Mazowieckim przy ul. Bartniaka wraz z niezbędną infrastrukturą i zagospodarowaniem, jest kompletny i został wykonany zgodnie z obowiązującymi przepisami oraz zasadami wiedzy technicznej.

imię i nazwisko	funkcja / uprawn.	branża	podpis
mgr inż. Sławomir Radziszewski specjalność elektryczna	projektant MAZ/0540/POOE/14	instalacyjna elektryczna	
mgr inż. Mirosław Konca specjalność elektryczna	sprawdzający CIE13/86	instalacyjna elektryczna	

2 Uprawnienia i zaświadczenia

3 Decyzja na lokalizację urządzeń w pasie drogi teletechnika

4 Pismo uzgodnienia przyłącze teletechnicznego Orange

5 Uzgodnienie przyłącze teletechnicznego Orange
